TASK ORDER (TO)

47QFCA19F0028

Travel Issuance and Overseas Citizen Assistance (TIOCA)

in support of:

Department of State (DOS)
Bureau of Consular Affairs (CA)
Office of Consular Systems and Technology (CST)

Issued to:
Deloitte Consulting, LLC

Conducted under Federal Acquisition Regulation (FAR) 16.505

Issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW (QF0B)
Washington, D.C. 20405

September 21, 2020
Modification 09

FEDSIM Project Number 2019020SD

Task Order **47QFCA19F0028 – Mod 9**

B.1   GENERAL

The work shall be performed in accordance with all sections of this Task Order (TO) and the contractor's basic contract, under which the resulting TO will be placed. A supporting acronym listing is included in Section J, Attachment A2.

B.2   CONTRACT ACCESS FEE (CAF)

The General Services Administration's (GSA) operating costs associated with the management and administration of this contract are recovered through a CAF. In accordance with the Alliant 2 base contract, the CAF shall be 0.75 percent of the total TO value with a cap of $100,000 per year per order (when order is in excess of $13.3M per order year). This TO shall have a separate Contract Line Item Number (CLIN) to cover this access fee, and this CAF shall be obligated at TO Award (TOA).

B.3   ORDER TYPES

The contractor shall perform the effort required by this TO on a Cost-Plus-Award-Fee (CPAF) basis for mandatory CLIN 0001 and optional CLINs 1001, 2001, 3001, 4001, 5001, and 6001 and a Not-to-Exceed (NTE) basis for CLINs 0002, 0003, 0004, 1002, 1003, 1004, 2002, 2003, 2004, 3002, 3003, 3004, 4002, 4003, 4004, 5002, 5003, 5004, 6002, 6003, and 6004.

B.4   SERVICES AND PRICES/COSTS

Long-distance travel is defined as travel over 50 miles from Washington, D.C. Local travel will not be reimbursed.

The following abbreviations are used in this price schedule:

CAF	Contract Access Fee
CLIN	Contract Line Item Number
CPAF	Cost-Plus-Award-Fee
NTE	Not-to-Exceed
ODC	Other Direct Cost
QTY	Quantity

B.4.1 BASE PERIOD

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
0001	Labor (Tasks 1-5) (b) (4)			

COST-REIMBURSEMENT TRAVEL and ODC/TOOLS CLINs

CLIN	Description		Total NTE Price
0002	Long-Distance Travel Including Indirect Handling Rate (b) (4)	NTE	(b) (4)
0003	ODCs and Tools Including Indirect Handling Rate (b) (4)	NTE	

CAF

CLIN	Description		Total Ceiling Price
0004	CAF	NTE	$100,000

TOTAL CEILING BASE PERIOD CLINs: (b) (4)

B.4.2 FIRST OPTION PERIOD

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
1001	Labor (Tasks 1-5)	(b) (4)		

COST-REIMBURSEMENT TRAVEL and ODC/TOOLS CLINs

CLIN	Description		Total NTE Price
1002	Long-Distance Travel Including Indirect Handling Rate (b) (4)	NTE	(b) (4)
1003	ODCs and Tools Including Indirect Handling Rate (b) (4)	NTE	

CAF

CLIN	Description		Total Ceiling Price
1004	CAF	NTE	(b) (4)

TOTAL CEILING FIRST OPTION PERIOD CLINs: (b) (4)

B.4.3 SECOND OPTION PERIOD

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
2001	Labor (Tasks 1-5)	(b) (4)		

COST-REIMBURSEMENT TRAVEL and ODC/TOOLS CLINs

CLIN	Description		Total NTE Price
2002	Long-Distance Travel Including Indirect Handling Rate (b) (4)	NTE	(b) (4)
2003	ODCs and Tools Including Indirect Handling Rate (b) (4)	NTE	

CAF

CLIN	Description		Total Ceiling Price
2004	CAF	NTE	(b) (4)

TOTAL CEILING SECOND OPTION PERIOD CLINs: (b) (4)

B.4.4 THIRD OPTION PERIOD

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
3001	Labor (Tasks 1-5)	(b) (4)		

COST-REIMBURSEMENT TRAVEL and ODC/TOOLS CLINs

CLIN	Description		Total NTE Price
3002	Long-Distance Travel Including Indirect Handling Rate (b) (4)	NTE	(b) (4)
3003	ODCs and Tools Including Indirect Handling Rate (b) (4)	NTE	

CAF

CLIN	Description		Total Ceiling Price
3004	CAF	NTE	(b) (4)

TOTAL CEILING THIRD OPTION PERIOD CLINs: (b) (4)

B.4.5 FOURTH OPTION PERIOD

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
4001	Labor (Tasks 1-5)	(b) (4)		

COST-REIMBURSEMENT TRAVEL and ODC/TOOLS CLINs

CLIN	Description		Total NTE Price
4002	Long-Distance Travel Including Indirect Handling Rate (b) (4)	NTE	(b) (4)
4003	ODCs and Tools Including Indirect Handling Rate (b) (4)	NTE	

CAF

CLIN	Description		Total Ceiling Price
4004	CAF	NTE	(b) (4)

TOTAL CEILING FOURTH OPTION PERIOD CLINs: (b) (4)

B.4.6 FIFTH OPTION PERIOD

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
5001	Labor (Tasks 1-5)	(b) (4)		

COST-REIMBURSEMENT TRAVEL and ODC/TOOLS CLINs

CLIN	Description		Total NTE Price
5002	Long-Distance Travel Including Indirect Handling Rate (b) (4)	NTE	(b) (4)
5003	ODCs and Tools Including Indirect Handling Rate (b) (4)	NTE	

CAF

CLIN	Description		Total Ceiling Price
5004	CAF	NTE	(b) (4)

TOTAL CEILING FIFTH OPTION PERIOD CLINs:

B.4.7 SIXTH OPTION PERIOD

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
6001	Labor (Tasks 1-5)	(b) (4)		

COST-REIMBURSEMENT TRAVEL and ODC/TOOLS CLINs

CLIN	Description		Total NTE Price
6002	Long-Distance Travel Including Indirect Handling Rate (b) (4)	NTE	(b) (4)
6003	ODCs and Tools Including Indirect Handling Rate (b) (4)	NTE	

CAF

CLIN	Description		Total Ceiling Price
6004	CAF	NTE	(b) (4)

TOTAL CEILING SIXTH OPTION PERIOD CLINs: (b) (4)

GRAND TOTAL CEILING ALL CLINs: $431,209,272

B.5 SECTION B TABLES

B.5.1 INDIRECT/MATERIAL HANDLING RATE

Long-Distance Travel and ODC/Tools costs incurred may be burdened with the contractor's indirect/material handling rate in accordance with the contractor's disclosed practices, provided that the basic contract does not prohibit the application of indirect rate(s) on these costs.

    a. If no indirect/material handling rate is allowable in accordance with the contractor's disclosed practices, no indirect/material handling rate shall be applied to or reimbursed on these costs.

    b. If no rate is specified in the schedule of prices above, no indirect rate shall be applied to or reimbursed on these costs.

The indirect handling rate over the term of the TO shall not exceed the rate specified in the schedule of prices above.

B.5.2 DIRECT LABOR RATES

Labor categories proposed shall be mapped to existing Alliant 2 labor categories.

B.5.3 INCREMENTAL FUNDING LIMITATION OF GOVERNMENT'S OBLIGATION

Incremental funding in the amount of **$73,450,758** for CLINs **0001 - 1004** is currently allotted and available for payment by the Government. Additional incremental funding for these CLINs may be allotted and available for payment by the Government as the funds become available. The estimated period of performance covered by the allotments for the mandatory CLINs is from award through **November 20, 2020**, unless otherwise noted in Section B. The TO may be modified to add funds incrementally up to the maximum of $431,209,272 over the performance period of this TO. These allotments constitute the estimated cost for the purpose of Federal Acquisition Regulation (FAR) Clause 52.232-22, Limitation of Funds, which applies to this TO on a CLIN-by-CLIN basis.

Incremental Funding Chart for CPAF

See Section J, Attachment A3.

B.6 AWARD FEE RESULTS REPORTING TABLE

The Award Fee Determination Plan (AFDP) establishes award fee. See Section J, Attachments A4 and A5.

C.1 BACKGROUND

The Department of State's (DOS's) Bureau of Consular Affairs (CA) is charged with protecting and assisting United States (U.S.) citizens abroad, issuing passports to U.S. citizens, and issuing immigrant and non-immigrant visas to foreign nationals according to the laws of the U.S. Government. The Office of Consular Systems and Technology (CST) within CA develops, deploys, and supports complex Information Technology (IT) systems and infrastructure that serve as the foundation of achieving CA's mission at domestic sites and overseas posts. CST delivers global technology solutions and provides comprehensive support to all customers and stakeholders.

Within CST, the Production Services Design and Development (PSDD) Division is charged with overseeing systems development and maintenance activities for citizen, non-citizen, and management systems. PSDD is also responsible for developing and maintaining production application software, business intelligence and reporting tools, and websites that support the mission of CA.

CA/CST develops, deploys, and supports complex IT solutions to automate the functions for the Department from concept to product, including research, design, development, testing, deployment, and production support. CA/CST also develops and implements standards for the Bureau's Enterprise Architecture (EA), maintains large-scale central data warehouses for real-time access to visa and passport records worldwide, monitors data quality, ensures system architecture meets current and projected requirements, and applies leading-edge technology solutions for systems' performance and security. CST strives to continuously provide innovative, global solutions that allow intuitive access to information services while balancing U.S. security and economic prosperity.

Travel Issuance and Overseas Citizen Assistance (TIOCA) is comprised of the following four functional programs, also referred to as the "TIOCA portfolio":

Passport Support Services (PSS):

Within CA, the Passport Services Directorate (CA/PPT) is responsible for the adjudication of U.S. citizenship and nationality, determination of entitlement, and issuance of passport documents to eligible U.S. citizens and nationals to facilitate trade, travel, and tourism. PSS systems provide technology supporting CA/PPT mission processes.

American Citizen Services (ACS):

Within CA, the Office of Overseas Citizen Services (CA/OCS) is responsible for providing a wide variety of services to American citizens residing or traveling abroad including, but not limited to, citizenship adjudication and passport issuance/renewal, Consular reports of birth or death abroad, travel registration services, welfare/whereabouts inquiries, services for citizens held in detention/arrest overseas, and financial transactions (e.g., loans, trusts, etc.). ACS systems provide technology supporting CA/OCS mission processes.

Non-Citizen Services (NCS):

Within CA, the Office of Visa Services (CA/VO) is responsible for the adjudication and issuance of visas to foreign nationals desiring to enter the U.S. as visitors or workers or to immigrate with

the intent of becoming permanent residents or citizens. NCS systems provide technology supporting CA/VO mission processes.

Consular Lookout and Support Systems (CLASS):

CLASS is used by DOS passport agencies, posts, and border inspection agencies to perform biographic matching on visa and passport applicants to identify individuals who may be ineligible for issuance or require other special action.

C.1.1 PURPOSE

The purpose of this TO is to obtain services for the PSS, ACS, NCS, and CLASS programs that include custom application software maintenance, Tier III support, and enhancements for legacy systems and tools. Enhancements will be limited to those required by law or executive mandates and to non-mandated enhancements for bug and security fixes, patches, and operational efficiencies. Enhancements include development and testing, as well as deployment preparation prior to deployment and verification that changes are fully functioning in the production environment as intended without adverse impact to the production environment.

An additional purpose of this TO is to provide linguistic expertise in the development and support of decision-support systems and name-matching/biographic matching algorithms, professional services to develop and manage application development of the name-matching systems, and systems architecture and maintenance support.

C.1.2 AGENCY MISSION

The mission of the U.S. DOS is to shape and sustain a peaceful, prosperous, just, and democratic world and foster conditions for stability and progress for the benefit of Americans and people everywhere. To achieve this DOS mission, CA actively pursues business, technology, and management enhancements and improvements.

C.2 SCOPE

CA/CST requires the contractor to provide maintenance and enhancement support. The scope of this TO includes, but is not limited to, the following products and services:

For the TIOCA Portfolio
   a. Program support.
   b. Project management.
   c. Production support.
   d. Tier III Help Desk support.
   e. Standard Operating Procedures (SOPs).
   f. Transition support from the incumbent contractor to the new contractor.
   g. Maintenance and enhancement support.
   h. Upgrades of selected applications to new application platform(s) or to other innovations.
   i. Software development and testing.
   j. Systems support training and knowledge transfer.
   k. Security.

    l.   Continuity and disaster recovery support.

For CLASS Program only

    m. Linguistic support and innovation.

    n. Sampling of linguistic data to ensure data quality.

The contractor shall be skilled in the databases, applications, and tools used by the TIOCA portfolio of systems, including the examples listed in Section J, Attachment A22.

CA/CST has adopted the Scaled Agile Framework (SAFe) approach for maintenance and engineering projects, when appropriate, and expects CA/CST services to flow using this approach. The contractor shall adhere to the CA/CST practices and guidelines accordingly.

Certain TIOCA portfolio legacy systems may be retired, in full or in part, during this TO period of performance. The TIOCA contractor shall maintain such systems up to the point of retirement. If CA/CST decides to retire any system, the TIOCA contractor shall supply documents and artifacts in accordance with CA/CST requirements. The contractor shall cooperate and coordinate with CA/CST in accounting for the full inventory of deliverables prior to completing any decommission process.

With respect to CLASS, the scope of this TO is for specialized linguistic computational support, application development, deployment, and database management. The contractor shall interact with DOS offices, other Government and non-government agencies, and other contractors as needed.

C.2.1 DEVELOPMENT, MAINTENANCE, TEST, AND PRODUCTION ENVIRONMENTS

The TIOCA contractor and IT systems that the TIOCA contractor uses shall cooperate and interoperate with other stakeholders that include CA/CST Government staff, the staff of other support contractors, and system users from various organizations.

The TIOCA contractor is responsible for software maintenance but not hardware maintenance. Maintenance of custom software includes re-design, revision and compilation of source code, configuration, debugging, testing, and quality control but does not include the development of new application systems. Maintenance of commercial software - such as operating systems, data base management systems, compilers, libraries, and other similar COTS tools - includes configuration and testing but not design or development.

Exogenous maintenance and enhancement requirements will arise over the life of the TO, e.g., new or revised guidelines or mandates from the Office of Management and Budget (OMB), Government Accountability Office (GAO), or other oversight organizations. As new applications systems undergo development, test, and eventual deployment into operations, the TIOCA contractor shall support the interoperability and compatibility of IT systems in the TIOCA portfolio with these new systems. Testing new application system modules shall sometimes require the TIOCA contractor's participation and support with respect to the TIOCA portfolio systems.

As new application functionality, systems, subsystems - such as ConsularOne[1] subsystems - are deployed, the TIOCA portfolio applications, including their APIs and other interfaces with the evolving ConsularOne constellation, will also require ongoing maintenance throughout the life of the TO.

DOS has contracted separately for the development of new application systems, including, principally, ConsularOne. The development, test, and use of these new application systems are outside the scope of the TIOCA TO. The TIOCA contractor shall decommission legacy application software systems in the TIOCA portfolio primarily due to their replacement by subsystems of the ConsularOne system, subsystems that are outside the scope of the TIOCA TO.

Maintenance, required enhancements, and decommissioning of TIOCA portfolio systems are the TIOCA contractor's responsibility. The contractor shall conduct all development and testing in the environment specified by the Government.

The TIOCA contractor is not responsible for production systems, except when the TIOCA contractor is required to resolve a Tier III Help Desk ticket that involves a production system. In that case, a solution developed by the TIOCA contractor will be installed on the production system by another party. Production systems run application software. Maintenance and enhancement of application software is the TIOCA contractor's responsibility.

The TIOCA TO scope includes, but is not limited to, the following:

a. Maintenance of the Government-Furnished Property (GFP) system software configuration in compliance with all CA, Diplomatic Security (DS), Information Resources Management (IRM), and DOS requirements such as virus definition updates, site iPost scores, and security updates (excluding maintenance of production hardware).

b. Operating system support to the GFP hardware located in the TIOCA contractor's secure facility, including tools and applications to maintain compatibility with the operating system when the OS is patched, reconfigured, or upgraded to a new version. Production hardware and the non-production environment (NPE) are managed outside the scope of the TIOCA TO. NPE and production hardware are *not* located at the TIOCA contractor's secure facility. The TIOCA contractor is not responsible for maintenance, patching and system administration for assets in the NPE boundary. However, the NPE is the environment where the TIOCA contractor will conduct all software development and testing activities. The TIOCA contractor will be a key user of the NPE

c. Database management support related to contractor-site GFP and cooperative efforts with other TOs and projects that use or interoperate with databases that the TIOCA contractor hosts or supports.

d. Platform support of contractor-site GFP. This includes platform upgrades of systems and application development systems. This also includes support to enable new or different types of computers and peripherals to be configured and tested prior to their deployment for production use. However, support of the production hardware itself is outside the scope of the TIOCA TO.

---

[1] Also known as "ConsularOne Applications and Data" (CA CAD)
https://www.state.gov/documents/organization/283674.pdf

e. Support of the DOS Independent Verification and Validation (IV&V) team, other contractors, and the Foreign Service Institute (FSI) to set up and configure applications and provide data and technical support as needed. This is applicable to the NPE but excludes management of all production hardware.

f. Assessment and Authorization (A&A) activity support, including but not limited to review and updates to system security documents and diagrams and participation in meetings. The TIOCA contractor shall conduct their own application security vulnerability testing during development. The TIOCA contractor shall remediate security vulnerabilities identified from security tests from all sources. It excludes scanning of servers or workstations, submission of documentation to Information Assurance (IA), or IA's assessment.

g. Site development documentation and code versioning support, including executables and source code, and check in of all files into the Configuration Control (CC) repository in accordance with CA/CST guidance. Excludes CC management and maintenance of the repository. See Section J, Attachment A28.

C.3   CURRENT IT AND NETWORK ENVIRONMENT

CA/CST IT systems are critical to the timely processing of passport and visa applications with the requisite level of accuracy and security that is essential to operating in the post-9/11 environment. Consular systems are installed at more than 300 consular processing facilities world-wide (embassies, consulates, domestic visa centers, or passport agencies, etc.), with approximately 7,000 consular staff users. Additionally, a total of approximately 11,000 DOS users and approximately 19,000 interagency users access these databases on a regular basis. They are central components to the core Departmental mission of protecting U.S. citizens while overseas, facilitating the legitimate travel of U.S. citizens, and ensuring proper U.S. entry of foreign nationals.

Samples of technical materials describing certain current aspects of the CA/CST IT and Network environment are in the attachments (Section J, Attachments A22 through A34). Applicable regulations, standards, and guidelines include those listed in Section J, Attachment A35.

In addition, the contractor shall:

a. Cooperate with inquiries by the DOS Office of the Inspector General (OIG) and the GAO.
b. Manage the workload; allow for surges in activities and varying product priorities.
c. Provide a standards-based, best practices approach to providing the services and support based on the Capability Maturity Model Integration (CMMI). The contractor shall maintain at least CMMI Level III DEV ratings for the duration of the TO.
d. Provide technical expertise (e.g., via participation in meetings, document reviews, ad hoc requests for information related to the systems covered in the TIOCA TO, and by recommending innovative technologies and methods within the scope of the TO).

C.4   OBJECTIVE

The objective of the TIOCA TO is to support CA/CST's systems while continuously improving, coordinating with others, and demonstrating efficiencies.

CA/CST requires significant coordination and communication of plans and activities by the contractor with customers and other contractors working under other TOs. Work performed shall be effectively coordinated and synchronized with work being performed under other TOs to ensure that customer requirements are met.

All hardware and software operated under the TO shall comply with CA/CST policies, directives, Standard Configuration Documents (SCDs), security configuration guidelines, and vendor-recommended patch levels. An inventory of all application software systems operated under the TO shall be maintained and include an accurate accounting of each system's compliance status with regard to operation, configuration, and security requirements.

C.5 TASKS

C.5.1 TASK 1 – PROVIDE PROJECT MANAGEMENT

The contractor shall provide project management support under this TO. This includes, but is not limited to, the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS).

C.5.1.1 SUBTASK 1.1 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a Project Kick-Off Meeting at a location approved by the Government (Section F, Deliverable 2). The meeting shall provide an introduction between contractor and Government personnel who shall be involved with the TO. The meeting shall provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include Key contractor Personnel, representatives from the directorates, other relevant Government personnel, the FEDSIM COR, and the CA/CST Government Technical Managers (GTMs).

At least three days prior to the Kick-Off Meeting, the contractor shall provide a Kick-Off Meeting Agenda (Section F, Deliverable 1) for review and approval by the FEDSIM COR and the GTMs prior to finalizing. The agenda shall include, at a minimum, the following topics/deliverables:

a. Points of Contact (POCs) for all parties.
b. Personnel discussion (i.e., roles, responsibilities, and lines of communication between contractor and Government).
c. Staffing Plan and status.
d. Transition-In Plan (Section F, Deliverable 16) and discussion.
e. DOS IT requirements (OpenNet, Government-Furnished IT, etc.)
f. Security discussion and requirements (e.g., building access, badges, Common Access Cards (CACs)).
g. Invoicing requirements.
h. Draft Project Management Plan (PMP) (Section F, Deliverable 8).
i. Updated Baseline Quality Management Plan (QMP) (Section F, Deliverable 13).
j. Earned Value Management (EVM) Plan.

k. Formal security briefing. (The Government will conduct a formal security briefing for the contractor (Section H.4.k). The purpose of the briefing will be to bring to the contractor's attention the governing documents and directives regarding all security considerations in the staffing of the project, site access, software and hardware functions, document control, and DOS procedures.)

The Government will provide the contractor with the number of Government participants for the Kick-Off Meeting, and the contractor shall provide sufficient copies of the presentation for all present.

The contractor shall provide a Kick-Off Meeting Minutes Report (Section F, Deliverable 3) documenting the Kick-Off Meeting discussion and capturing any action items.

C.5.1.2 SUBTASK 1.2 – PREPARE A CONTRACT STATUS REPORT (CSR)

The contractor shall provide a monthly CSR that includes the information depicted in Section J, Attachment A6 (Section F, Deliverable 5).

C.5.1.3 SUBTASK 1.3 – CONVENE CSR STATUS MEETINGS

The contractor Program Manager (PM) shall convene a monthly CSR Status Meeting with the CA/CST GTM, FEDSIM COR, and other Government stakeholders (Section F, Deliverable 6), or more frequently when events so warrant. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and the CSR, provide opportunities to identify other activities, establish priorities, and coordinate resolution of identified problems or opportunities. The contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the GTMs and FEDSIM COR (Section F, Deliverable 7).

C.5.1.4 SUBTASK 1.4 – PROVIDE ALTERNATIVE EARNED VALUE MANAGEMENT (EVM) METRICS AND CALCULATION SUPPORT

The contractor shall employ and report on EVM type metrics and calculations in the management of this TO as described in this section of the TO. The Government expects the contractor to employ innovation in its proposed support for this subtask and TO in accordance with best industry practices. The following information shall be included in each CSR (Section F, Deliverable 5) as outlined in the Project Management Plan (PMP).

a. Planned Work (PW)
b.   Actual Work (AW)
c. Actual Cost (AC)
d. Planned Cost (PC)
e.   Burndown Chart
f. A variance analysis that includes the following:
  1. Cost Variance (CV) = (PC - AC)
  2. Cost Variance % = (CV/PC X 100%)
  3. Cost Performance Index (CPI) = (PC/AC)
  4. Schedule Variance (SV) = (AW-PW)

    5.   Schedule Variance % = (SV/PW X 100%)

    6.   Schedule Performance Index (SPI) = (AW/PW)

f. Explain all variances greater than ten percent.

g. Explain, based on work accomplished as of the date of the report, whether the performance goals will be achieved.

h. Discuss the corrective actions that will be taken to correct the variances, the risk associated with the actions.

C.5.1.5 SUBTASK 1.5 – PREPARE AND UPDATE THE PROJECT MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a PMP. The contractor shall provide the Government with a draft PMP (Section F, Deliverable 8) on which the Government will make comments. The final PMP (Section F, Deliverable 9) shall incorporate the Government's comments.

The PMP shall:

a. Describe the proposed management approach.

b. Contain detailed SOPs for all tasks (Section F, Deliverable 23).

c. Include milestones, tasks, and subtasks required in this TO.

d. Provide an overall Work Breakdown Structure (WBS) with a minimum of three levels and associated responsibilities and partnerships between Government organizations.

e. Describe in detail the contractor's approach to risk management under this TO.

f. Describe in detail the contractor's approach to communications, including processes, procedures, communication approach, and other rules of engagement between the contractor and the Government.

g. Plan for compliance with A&A, Authority to Operate, and other security requirements.

h. Include the contractor's updated QMP (Section F, Deliverable 13), see C.5.1.5.1., and the Alternative EVM Metrics and Calculations Support Plan.

i. Conform to the Project Management Body of Knowledge (PMBOK).

The contractor shall provide project schedules to be integrated with CA/CST's Integrated Master Schedule (IMS). IMS aggregates individual schedule inputs from multiple projects to aid sequencing project tasks in an optimal order to meet CA/CST's overall priorities. The IMS is a vehicle for analysis and management of dependencies between projects, resource utilization, identification of resource constraints, and prioritization of activities across the enterprise.

Management of the CST IMS is not within the scope of this TO. Each project schedule will be maintained and updated to reflect progress after each FEDSIM COR and CA/CST GTM status update, review, or milestone change.

The PMP is an evolutionary document that is to be updated annually at a minimum (Section F, Deliverable 10). The contractor shall work from the latest Government-approved version of the PMP.

C.5.1.5.1 SUBTASK 1.5.1 – PROVIDE QUALITY MANAGEMENT

The contractor shall identify and implement its approach for providing and ensuring quality throughout its solution to meet the requirements of the TO. The contractor's QMP shall describe the application of the appropriate methodology (e.g., Quality Control (QC) and/or Quality Assurance (QA)) for accomplishing TO performance expectations and objectives. The QMP shall describe how the appropriate methodology integrates with the Government's requirements.

Offerors shall submit the draft QMP with its proposal. The contractor shall update the QMP and submit it with the PMP at the Kick-Off Meeting (Section F, Deliverable 13). The Government will provide comments on the updated QMP. The Contractor shall incorporate the Government's comments and provide the Final QMP (Section F, Deliverable 14). The contractor shall periodically update the QMP (Section F, Deliverable 15) as changes in program processes are identified.

C.5.1.6 SUBTASK 1.6 – PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report when the request for travel is submitted (Section F, Deliverable 11). The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and POC at travel location. Trip reports shall also contain Government approval authority, total cost of the trip, a detailed description of the purpose of the trip, and any knowledge gained. At a minimum, trip reports shall be prepared with the information provided in Section J, Attachment A8.

C.5.1.7 SUBTASK 1.7 – TRANSITION-IN

The contractor shall update the draft Transition-In Plan (Section F, Deliverable 16) provided with its proposal and provide a final Transition-In Plan (Section F, Deliverable 17) as required in Section F. The contractor shall ensure that there will be minimal disruption to vital Government business and no service degradation during and after transition. The contractor shall implement its Transition-In Plan at Project Start, and *all* transition activities shall be completed 120 calendar days after approval of the final Transition-In Plan (Section F, Deliverable 17).

C.5.1.7.1 WORK AND NETWORK ACCESS DURING TRANSITION-IN

The Transition-In period will allow most technical team members on the incoming TO staff to obtain badges and RSA tokens and connect to OpenNet, the Department's non-classified information system.

The Global OpenNet (GO) network, accessed via RSA token, provides web-based access to OpenNet and OpenNet-based systems (such as most of the Microsoft Office Suite, including Outlook) and will allow some technical work to be done for production support and limited development work via the NPE. However, access to databases for production support is not available through GO; the contractor must have a direct OpenNet connection.

Direct OpenNet connection is provided via a dedicated line or bandwidth and network drops. This requires an inspection of the premises and approval by Diplomatic Security (DS) before OpenNet connections can be installed. (See Section H.4.2 and https://go.state.gov regarding OpenNet.)

Pending a direct OpenNet connection, no technical work will be possible without GO and RSA tokens. Thus, remote access for teleworking or after hours support via GO will be limited during Transition-In.

The initial installation of GFP, including specialized printers, will be completed during the Transition-In.

C.5.1.8   SUBTASK 1.8 – TRANSITION-OUT

The contractor shall provide Transition-Out support when required by the Government. The Transition-Out Plan shall facilitate a smooth transition from the incumbent to incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a draft Transition-Out Plan within eight months of Project Start (PS) (Section F, Deliverable 18). The Government will work with the contractor to finalize the Transition-Out Plan (Section F, Deliverable 18). At a minimum, the contractor shall review and update this Plan annually (Section F, Deliverable 19). Additionally, the Transition-Out Plan at least quarterly during the final Option Period (Section F, Deliverable 20).

The Transition-Out Plan shall identify how the contractor coordinates with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

a.   Project management processes.
b.   POCs.
c.   Location of technical and project management documentation.
d.   Status of ongoing technical initiatives.
e.   Appropriate contractor-to-contractor coordination to ensure a smooth transition.
f.   Transition of Key Personnel.
g.   Schedules and milestones.
h.   Actions required of the Government.

The contractor shall maintain effective communication with the incoming contractor/ Government personnel for the period of the transition via weekly status meetings and as often as necessary to ensure a successful transition-out.

The contractor shall implement its Transition-Out Plan NLT six months prior to TO expiration.

C.5.1.9   SUBTASK 1.9 – PREPARE A QUARTERLY SPEND PLAN

The contractor shall submit and maintain a Quarterly Spend Plan (Section F, Deliverable 21) that reflects the projected spending for the upcoming 12 months. This shall include a detailed break out of the following:

a.   Task
b.   CLIN Number
c.   Contractor Function/Role
d.   Employee Status (exempt, non-exempt, subcontractor)
e.   Employee Name
f.   Alliant 2 Labor Category

g. Subcontractor(s) Company Name(s), if applicable

h. Hours and Dollars per contractor function/role for each option period and month within the option period

i. Rate information (i.e., burden and unburdened) for each respective plan month

j. Totals of hours and costs by CLIN and Task Number

k. Non-Labor Costs

l. Grand Total hours/Costs by Task Number

C.5.1.10   SUBTASK 1.10 – PREPARE A WEEKLY ACTIVITY REPORT

The contractor shall prepare and submit a Weekly Activity Report (Section F, Deliverable 4) in accordance with the provided template, Section J, Attachment A7, and addressing all four TIOCA portfolio programs and systems.

C.5.2   TASK 2 – PRODUCTION SUPPORT

Task 2 Production Support includes support for all TIOCA portfolio systems.

C.5.2.1   TASK 2.1 – TIER III HELP DESK SUPPORT

The contractor shall provide Tier III Help Desk support for the TIOCA portfolio systems in accordance with performance standards (Section J, Attachments A4 and A5).

The contractor shall:

a. Troubleshoot system problems that cannot be resolved by the on-site systems management personnel or end-user support personnel, including the Tier I and Tier II Help Desks, which are provided by resources other than the TIOCA contractor.

b. Accept tickets via the CA/CST ticket system, email, or phone and open a ticket if one does not exist.

c. Support critical and high tickets/problems by being available on-call during non-business hours 24 x 7 and provide a telephone number. All problems reported via tickets will be resolved within the established standards.

d. Use the CA/CST ticket system to manage tickets and to calculate Help Desk metrics.

e. Provide SOPs and training staff to complete handoff of routine production support issues.

The contractor's support team shall be available on-call during non-business hours and weekends (24 hours per day, seven days per week (24 x 7)).

C.5.2.2   TASK 2.2 – APPLICATION ADMINISTRATION – PRODUCTION CONTROL

The contractor shall provide production support for the four programs and their subsystems as follows:

a. Coordinate with the Configuration Management (CM) and Government deployment team to move all documents, source code, etc. to the production environment (Section F, Deliverable 24).

b. Provide production control schedules in coordination with CA Service Operations.

c. Create scripts to execute batch processes.

d. Create operational memos and job requests.

e. Support the creation of the Release Task List (RTL).

f. Review each release package for completeness before submission for formal acceptance or rejection by the Government.

g. Deposit all CM products and intellectual knowledge in the central CA/CST CM repository.

h. Stage and support the implementation of software releases.

i. Manage security and IA compliance (C.5.2.5.1, C.5.2.5.2).

j. Perform patch management and security update operations support (C.5.2.5.3, C.5.2.5.4, C.5.2.5.5).

C.5.2.3   SUBTASK 2.3 – STANDARD OPERATING PROCEDURES (SOPs)

Based on best practices, lessons learned, and/or new innovations (Section F, Deliverable 23), the contractor shall:

a. Develop new SOPs, including SOPs for frequently repeated processes (such as onboarding steps and requests for access or server setup).

b. Review and update existing SOPs at a minimum annually or as needed.

c. Maintain and manage the SOP Library in Government-sponsored repositories (e.g., on OpenNet).

d. Maintain version control.

e. Demonstrate continued, routine use of SOPs in performing work.

f. Ensure operational procedures are documented and approved and user manuals are complete.

g. Document unit test plans and results.

SOP development and revision is applicable to all four TIOCA portfolio programs.

C.5.2.4   SUBTASK 2.4 – STREAMLINE OPERATIONS AND MINIMIZE OPERATIONAL COSTS

The contractor shall recommend approaches to the Government for meeting all contract requirements. These approaches are to maximize efficiency, streamline operations, improve results, strengthen security, and minimize operational costs (all four programs and systems).

Streamlining approaches may include, but are not limited to:

a. Revised, innovative implementation of industry standard frameworks such as Information Technology Infrastructure Library (ITIL), CMMI, and PMBOK, including migration to new versions as they arise.

b. Revision of existing SOPs (e.g., revisions to the Legacy System Enhancement Process (Section J, Attachment A26)); ongoing revision to the CA/CST Scaled Agile Process (Attachment A30); generate new version(s) of the Application and Coding Testing Standards generally, new Code Quality (CQ) analyses or Continuous Integration and Continuous Delivery (CI/CD) tools and processes within that standard.

c. New versions, documentation, and/or revision of other existing standards, analyses, or processes to reflect evolving industry practice, streamline operations, improve results, strengthen security, or minimize costs.

C.5.2.5 SUBTASK 2.5 – SECURITY TASKS

C.5.2.5.1 SECURITY OPERATIONS

The contractor shall comply with Departmental security policies and procedures, as outlined in the Foreign Affairs Manual (FAM) and the Foreign Affairs Handbook (FAH), including, but not limited to, 12 FAM, 12 FAH, and 5 FAH (reference Web site: https://fam.state.gov/default.aspx). The contractor shall manage security and IA compliance of all applications under the TIOCA TO, including relevant software upgrades for security compliance and use in production systems. In addition, the contractor shall be responsible for maintaining onsite GFP in accordance with Departmental security policies and procedures. Overall management of the CST Information Systems Security and Security Operations program is outside the scope of the TIOCA TO.

The contractor shall fully cooperate with DOS audits, reviews, evaluations, tests, and assessments of contractor systems, processes, and facilities. The contractor shall comply with Federal security controls including, but not limited to, those specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 4 or later. The contractor shall be responsible for keeping up to date with security controls relevant to the TIOCA portfolio applications.

The contractor shall provide support as requested by the Government when security tests are conducted by another organization to validate that required security controls are properly implemented, operate as intended, and produce the desired outcome. The TIOCA contractor shall remediate security vulnerabilities identified from security tests from all sources and shall assist in verification testing as requested. The contractor shall perform its own security testing as part of QA/QC while working on patch releases, enhancements, or configuration changes for the applications falling under the TIOCA portfolio, to ensure additional security vulnerabilities are not introduced in these products. (Please also reference C.5.3 and C.5.4.)

C.5.2.5.2 INFORMATION ASSURANCE (IA) AND COMPLIANCE SUPPORT

The contractor shall perform IA and compliance support services to maintain production system security posture, which includes engineering, implementing, operating, and monitoring. As noted above, another organization is responsible for the overall management of the Information System Security Office and the Security Operations program. Support includes implementing remediation actions as required, and providing timely and accurate input to documentation. Examples of support include but are not limited to:

a. Support the A&A process.
b. Security findings and remediation from all sources.
c. Security findings management and status reporting.
d. iPost findings and remediation, See
    https://2009-2017.state.gov/documents/organization/156865.pdf.
e. Group Policy Object (GPO) compliance.

    f.   Enclaving/network segregation.

The contractor shall maintain, manage, and report on all security findings falling under the scope of the TIOCA program, including engineering mitigations for findings from all sources as requested by the Government. The contractor shall maintain acceptable levels of security finding grade(s):

    a.   The contractor shall remediate and close open security finding items as agreed upon in the timeline listed in the Plan of Actions and Milestones (POA&M).

    b.   The contractor shall update open security finding items periodically as needed.

C.5.2.5.3 SECURITY OPERATIONS SUPPORT

The contractor shall support security operations by closely coordinating with the ISSO as well as the Security Operations organization, which are principally responsible for operational security administration. The contractor shall provide requirements for and assist in the configuration of CST's Security Information and Event Management (SIEM) system, as it pertains to the management of TIOCA portfolio applications. The contractor shall support responses and investigations into events and incidents as requested by the Government.

C.5.2.5.4 PATCH AND SECURITY UPDATE

The contractor shall perform patch management and security update operations support to maintain operating environments for their Organizational Units (OUs), which shall be comprised of GFP at the contractor facility. Responsibilities include, but are not limited to:

    a.   Providing oversight and periodic review of the patch management process and procedures at the TIOCA contractor facility.

    b.   Complying with required processes and procedures so that patches are successfully applied in TIOCA contractor OUs and are reported accurately.

    c.   Performing patch and security update deployment testing upon request.

    d.   Monitoring, reporting, and remediating all deployment failures within 24 hours.

    e.   Monitoring and reporting patch and security update compliance for all CA systems weekly.

    f.   Providing weekly, monthly, and/or as requested patch and security update status reports.

    g.   Communicating with all appropriate parties.

    h.   Complying with DOS rules and regulations governing patch and security update operations.

    i.   Maintaining an iPost score at or below the acceptable levels, as defined by DOS, for sites and operating environments maintained by the contractor.

    j.   Complying with DOS patch timeframe requirements in accordance with relevant Notification Bulletins.

C.5.2.5.5 CONTINUITY AND DISASTER RECOVERY

The contractor shall incorporate all aspects of the TIOCA portfolio systems into CST's Contingency of Operations (COOP)/Disaster Recovery Plan(s). The overall management of COOP/Disaster Recovery across CST is outside the responsibility of the TIOCA contractor.

However, the contractor shall be prepared to provide input into planning and testing as it pertains to TIOCA portfolio systems, as well as coordinating with the Government, when significant changes to the architecture occur. Responsibilities include but are not limited to:

a. Support facility contingency planning, disaster recovery, and testing, as needed.

b. Continually provide accurate and up to date input for support and continuity architecture documents and disaster recovery program documentation.

c. Continually provide accurate and up to date input for disaster recovery program documentation.

d. Continually provide accurate and up to date input for data recovery and COOP plans with standard failure detection and recovery procedures.

e. Continually provide accurate and up to date input for the CA/CST Redundancy Chart that tracks recovery options for each application, database and service managed by CA/CST.

f. Participate in disaster recovery tests across the enterprise and documenting results for TIOCA portfolio systems.

g. Coordinate with appropriate CST contractors and the Government to ensure disaster recovery capabilities are maintained as changes are made to systems and environments.

h. Support system and facility contingency planning, disaster recovery, and testing, as needed to support COOP/Disaster Recovery Planning (Note: providing a disaster recovery site is outside the scope of this TO).

C.5.2.6   SUBTASK 2.6 - TIOCA PORTFOLIO APPLICATIONS TRAINING

The contractor shall provide application-specific training support. This shall include briefings and demonstrations (Section F, Deliverable 24), including training other contractor and Government staff on how to conduct training of others (i.e., train the trainer). The contractor shall:

a. Support consular applications training courses by providing input into training materials as requested by CST. The contractor shall review and edit the training materials developed by the Training Team (not the TIOCA contractor). Training will be located in the Washington D.C. area.

b. Support the Department's Enterprise Training Environment (ETE) by verifying that the TIOCA portfolio applications are fully functioning, up-to-date, and operational in the training environment. Another contractor is responsible for the overall maintenance of the ETE environment.

C.5.3   TASK 3 – TIOCA PORTFOLIO SOFTWARE MAINTENANCE

CA/CST requires application support and ongoing software maintenance for TIOCA portfolio applications and systems (Section F, Deliverable 25) as well as deployment and transition support for system or software enhancements, upgrades, or architecture changes. Maintenance includes technical support, upgrading platforms and underlying software frameworks and component libraries, ensuring compatibility with upgraded operating systems, software maintenance, bug fixes and minor releases, training and documentation support, Tier III support, and emergency support as follows in the list below. Note, the TIOCA contractor will develop the

application platform upgrade solution and lead and facilitate the deployment, but the upgrade will in most cases be executed by another contractor. (See Section C.3 and Attachments A22 through A35 regarding standards and methods.)

The contractor shall:

a. Maintain and manage distributed system applications' software, including software development of changes as mandated and approved.

b. Coordinate with CA/CST's Enterprise Architecture team, the Chief Engineer, and the data engineering teams to ensure compliance with the CA/CST target architecture.

c. Maintain and/or integrate web services using industry best practices and CA/CST-approved web service policies and guidelines.

d. Consult with other technical stakeholder teams (e.g., visa, passport, ConsularOne, and databases).

e. Provide support during installations at operational sites, ensure that operational procedures are documented and approved user manuals are complete, unit test plans and results are documented, and all training is delivered prior to turning over the system for operation.

f. Verify system reliability, availability, and maintainability. The contractor shall obtain reliability and availability data from the software vendors for a field-proven system; the contractor shall obtain these figures from an operational system.

g. Provide software development lifecycle documents and other intellectual property.

h. Draft features, user stories, or Change Control Requests (CCRs) (Section J, Attachment A28) based on identified system change needs and/or as needed.

i. Analyze Test Incident Reports (TIR) (Section J, Attachment A31) as problems are identified and provide recommendations to the COR and GTMs.

j. Provide technical support for the production environment in accordance with CCR guidelines.

k. Analyze maintenance requirements, mandates, and other changes, to include level of effort in terms of time (hours, days, weeks, etc.), duration and costs.

l. Implement software releases in accordance with CA/CST lifecycle governance processes as identified (Section C.3 and Attachments A22 through A35) (Section F, Deliverable 26).

m. Create, update, maintain, and use a knowledge database (currently on the Remedy platform) to ensure consistent, repeatable, and efficient response to support CA requests and allow end-users direct access for problem resolution.

C.5.3.1 SUBTASK 3.1 – TIOCA PORTFOLIO QUALITY ASSURANCE (QA) TESTING

The contractor is required to test any release for QA/QC to ensure that all functionality performs as specified in the requirements and that security vulnerabilities are not introduced in these products. The contractor shall also conduct thorough QA testing to ensure that rounds of IV&V testing and IV&V-generated functional and security defects are minimized as much as possible and that new issues and vulnerabilities are not introduced into production. The performance and functionality of the systems are the responsibility of the contractor. The contractor shall prevent

or overcome any problems in production that arise due to differences in the QA or IV&V environments.

The contractor shall work with other stakeholder teams to ensure that testing by the IV&V team is well coordinated and that testing schedules are kept on track as much as possible. This includes support for the IV&V environment set up and coordinating/collaborating with the Database Engineering Data Management (DEDM) team on data, scripts, and deployments.

The contractor shall:

a. Perform QA testing prior to IV&V testing.

b. Perform integration testing to ensure all system components work successfully together.

c. Automate testing and deployment processes to the extent possible, as approved by the Government.

d. Provide continuous regression testing in all environments and provide engineering and solutions to ensure the system functions in production.

e. Provide support of IV&V testing and address errors identified by IV&V.

f. Work with the Government to establish virtual development and testing environments on the NPE.

g. Perform prototyping as appropriate.

C.5.3.2 SUBTASK 3.2 – NON-EMERGENCY PATCH RELEASES

The contractor shall implement non-emergency patch and maintenance releases that include bug fixes, security and performance issues, and other modifications (Section F, Deliverable 26). The contractor shall work with the release management process established by CA/CST Service Strategy and Portfolio Management (SSPM) to schedule patch and maintenance releases to maximize efficiencies and minimize risks, unless an urgent fix is required by the Government (Section J, Attachments A28 and A32). The contractor shall ensure that these releases are fully functioning in the production environment as intended, meeting the release's acceptance criteria without adverse impact to the production environment.

The contractor shall deliver relevant system and implementation documentation (Section F, Deliverable 25) for patch and maintenance releases as defined in the SSPM project tailoring plan. Generally, updates to requirements, training, and system documents are required for functionality changes.

Implementation documentation is required for all releases and includes release notes, configuration requirements and deployment instructions. The contractor shall ensure that the customer is included in the release process and scheduled reviews. The contractor supports the following release activities:

a. Provide patch/maintenance releases for bug fixes, security patches, and/or minor system maintenance for CA/CST systems and applications that have been fully tested and ready for production.

b. Test hardware and peripheral configurations to ensure compatibility and interoperability.

c. Perform routine maintenance to keep all existing systems fully functional as long as they are needed.

d. Deliver software packages including documentation to CM; assist CM in deploying application in the NPE and complete contractor integration and configuration testing in this production-like environment.

e. Fix performance, security, and code issues identified by the Government in NPE. The Government plans to use static code analysis to identify issues and will work with the contractor to determine required fixes before moving to IV&V.

f. Deliver systems and integrated tested software and documentation via CM to IV&V and support (e.g., bug fixes) independent testing as needed.

g. Conduct deployment activities for release of software to the field including installation on new and replaced or refreshed hardware. The TIOCA contractor shall develop the application patch release and installation guide. The TIOCA contractor will participate in the deployment meetings and perform any necessary smoke testing after the upgrade is completed by another contractor team.

h. Coordinate deployment activities closely with other teams as needed.

i. Draft CCRs based on identified system change needs.

j. Improve existing software to enhance performance.

k. Deliver contractor's internal QC/QA test results for releases.

l. Deliver implementation documentation for releases.

m. Manage and maintain schedule, scope, risks, issues, resources, and communication channels for releases.

n. Maintain offsite (contractor's secure facility) development and integrated testing environments.

o. Comply with CA/CST project management policies (Section C.3 and Attachments A22 through A35).

p. Support CA/CST configuration management process including using the configuration management repository for code, executables, and document management.

q. Participate in release meetings and collaborate with others to ensure successful operations and implementations.

C.5.3.3 SUBTASK 3.3 – TIOCA PORTFOLIO EMERGENCY PATCH RELEASES

The contractor shall implement emergency patches in coordination with the GTMs to remediate any CA/CST system or application security vulnerabilities, bug fixes, or correct system performance in an expedited manner. The contractor shall ensure that these releases are fully functioning in the production environment as intended, meeting the release's acceptance criteria, without adverse impact to the production environment.

The contractor shall perform emergency patch release activities in accordance with performance standards (Section J, Attachments A4 and A5). When an emergency patch is implemented, the patch shall be documented to the extent required by CST guidelines (Section F, Deliverables 26 and 29). The contractor shall deliver relevant system and implementation documentation for patch releases. Implementation documentation includes release notes, configuration requirements, and deployment instructions.

C.5.4   TASK 4 – TIOCA PORTFOLIO SOFTWARE ENHANCEMENT

The contractor shall provide software analysis, design, and enhancement support for components that may be required during the life of the TO to support the general TIOCA portfolio business area (Section F, Deliverable 27). The contractor is required to document enhancement requirements in coordination with the Government (Section F, Deliverable 28). The contractor shall ensure that these releases are fully functioning in the production environment as intended, meeting the release's acceptance criteria without adverse impact to the production environment. New components may be required as a result of initiatives with other agencies, congressional mandates, increased data sharing and data gathering with the general public, migration of consular automated systems to new development and/or operating platforms, remediation of security vulnerabilities, and to maintain alignment with the CA/CST EA. Software enhancements and modernization include, but are not limited to, the following:

a. Interface existing and legacy CA/CST systems to future CA/CST EA driven by legislation or as needed.
b. Develop new functionality or components for existing TIOCA portfolio systems or to replace/improve old functionality.
c. Develop new enhancement releases for existing TIOCA portfolio systems.
d. Migration of existing applications to new technical platform(s).
e. Perform data migration and decommission of legacy systems.
f. Provide transition support to migrate CA Extensible Markup Language (XML) interfaces to CA/CS National Information Exchange Model (NIEM) consistent interfaces or suitable alternative as needed.

All enhancements are subject to the Enhancement Request Process (Section J, Attachments A26 and A27) (Section F, Deliverable 28). The contractor may recommend revisions to the enhancement process (or other processes) (Section C.5.2.4).

Implementation of software releases shall be executed in accordance with CA/CST lifecycle governance processes (Section C.3 and Attachments A22 through A35) (Section F, Deliverables 27, 28, and 29).

C.5.5   TASK 5 – CLASS SUPPORT

The contractor shall provide specialized linguistic computational support and application development and support the deployment and database management teams. The contractor shall interact with DOS offices, other Government and non-government agencies, and other contractors as needed.

C.5.5.1   SUBTASK 5.1 – SPECIALIZED LINGUISTICS SUPPORT

The contractor shall provide specialized linguistics support, described below, in the following areas:

a. Name-Matching Algorithm Management
b. Query Results Accuracy Improvement
c. CLASS Training
d. Data Maintenance, Management, and Analysis

C.5.5.1.1 NAME-MATCHING ALGORITHM MANAGEMENT

The contractor shall provide linguists for operational systems support and to support application teams' ongoing software maintenance for name-checking algorithms, as well as deployment and transition support to future name-checking algorithms to be employed within CLASS (Section F, Deliverable 31). The contractor shall provide continuity in processes, activities, tools, and standards involved with operating, administering, managing, and maintaining name-checking algorithms. The contractor shall also provide linguistic support for the operation, maintenance, and enhancement of the name-checking systems. At a minimum, the contractor shall demonstrate a full understanding of the purposes of and approaches to name-check processing, as may be employed or needed by the DOS. The contractor shall:

a. Perform linguistic analysis of visa and passport message traffic relating to cultural name structures and name variants, review the "lookout" database to ensure correct system operation, and research new linguistic techniques for potential use in name-check processing. The contractor shall develop and field innovative, enhanced name-check and computational linguistics CLASS system algorithms and processes derived from academic, industrial, or other sources in the field.

b. Maintain Name-Checking Algorithm documentation (Section F, Deliverable 30) associated with CLASS, provide updates to the FAM, and provide input to the business offices for All Diplomatic and Consular Posts (ALDAC) cables.

c. Recommend, and if authorized, implement modifications to tuning parameters to correct problems or enhance the efficacy of the name-checking process.

d. Modify current linguistic algorithms and, as appropriate, develop new linguistic algorithms for the name-checking systems in order to improve accuracy of query results (Section F, Deliverable 31).

e. Support functional testing and QC activities.

f. Create a deployment and transition plan for new cultural, linguistic, or other algorithms. (Note: This requirement is driven by customer needs. It is estimated that there may be one over the whole life of the TO.)

g. Provide expert linguistic representation for CA at interagency and international meetings and activities.

h. Provide research support and maintain awareness of internal and external research efforts related to the name-check systems, including examination of name-check output reports.

C.5.5.1.2 QUERY RESULTS ACCURACY IMPROVEMENT

The contractor shall design and implement next generation CLASS functionality that increases the accuracy and usefulness of query results (Section F, Deliverable 32). At a minimum, the contractor shall evaluate and, if appropriate, recommend the following for incorporation into a development program for eventual implementation in CLASS:

a. Alternatives to rules-based data quality analysis and queries.

b. Original language searches and transition to Unicode.

c. Phonetic name searches.

d. Integration of additional culturally relevant information.

e. Additional integration of language family and subfamily to determine data relevance and importance.

f. Additional data fields or variables in improving query accuracy such as networks of names (known associates, etc.) or allowing for Also-Known-As (AKA) on fields other than name (e.g., Date of Birth).

g. Enhancements and innovations for prioritization of responses by severity or level of importance. This may include multiple severity factors that differ depending on the user base performing the query as well as significance of the query results (e.g., Category 1 versus administrative refusal).

h. Enhancements and innovations for prioritization of responses by the relevance, variations, and weighting of biographic information (Place of Birth, Date of Birth, Name, etc.).

i. Additional integration of the most appropriate applications of onomastics research and scholarship in the development and enhancement of linguistic algorithms (Section F, Deliverable 31).

j. Systems which use logic similar to CLASS but determine near-match situations regarding addresses, text, and/or phone numbers.

C.5.5.1.3 CLASS TRAINING

The contractor shall provide CLASS-specific training, briefings, and demonstrations, and shall provide expert linguistic support for the development of other training courses (Section F, Deliverable 33). This includes training Government staff how to conduct training of others (i.e., train-the-trainer).

The contractor shall:

a. Support the FSI's Basic Consular Course (CONGEN) development by reviewing the FSI course materials and providing updated CLASS content input/material on any changes to the environment as needed. This course is to train Junior Officers on how to use CLASS. FSI will develop the materials and teach the course.

b. Support the CLASS training courses other than CONGEN by maintaining, revising, and developing training materials and by providing the half-day training. The contractor shall submit training materials to the CST training team for review/concurrence. Training shall be located at FSI in the Washington, D.C. area approximately four times per year.

C.5.5.1.4 DATA MAINTENANCE, MANAGEMENT, AND ANALYSIS

The contractor shall maintain, manage, and analyze CLASS name-matching data. The contractor shall support ongoing data quality improvement activities and perform advanced mathematical and statistical data analyses to support specific Governmental initiatives.

Data Analysis

The contractor shall provide mathematical and statistical data analysis on all data processed by the CLASS name-check system. The contractor shall provide new and innovative mathematical modeling techniques to support various counter-terrorist and counter-fraud activities.

The contractor's data analysis shall:

a. Identify subtle patterns that indicate suspicious behavior warranting further investigation.
b. Determine what is expected in normal circumstances as compared to known fraudulent cases.
c. Detect fraud both in real time and for forensic determination.
d. Apply knowledge of CA systems, processes, and processing times to understand the significance of the results of each mathematical and statistical data analysis.

Data Quality and Management

The contractor shall provide data quality and management support of all data sources that provide input to CLASS.

The contractor shall:

a. Analyze data discrepancies and name-check inconsistencies, identify potential problems, and recommend improvements. These shall be included in the Weekly Activity Report (WAR) (Section F, Deliverable 4) (Section J, Attachment A7).
b. Document all name-check and data comparison findings and provide recommendations for name-check changes (Section F, Deliverable 4).
c. Prepare and disseminate statistical and data reports (Section F, Deliverable 4).
d. Conduct regular Data Management Group meetings among representatives of the Visa Office, Passport Office, and others to discuss data-related issues impacting all distributed travel document issuance systems.

This page intentionally left blank.

E.1   PLACE OF INSPECTION AND ACCEPTANCE

Inspection and acceptance of all work performance, reports, and other deliverables under this TO will be performed by the FEDSIM COR and CA/CST GTMs.

E.2   SCOPE OF INSPECTION

All deliverables will be inspected for content, completeness, accuracy, and conformance to TO requirements by the FEDSIM COR and CA/CST GTMs. Inspection may include validation of information or software through the use of automated tools, testing, or inspections of the deliverables, as specified in the TO. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables.

The Government requires a period NTE 15 workdays after receipt of final deliverable items for inspection and acceptance or rejection.

E.3   BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the TO and relevant terms and conditions of the TO. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

The final acceptance will occur when all discrepancies, errors, or other deficiencies identified in writing by the Government have been resolved, through documentation updates, program correction, or other mutually agreeable methods.

Reports, documents, and narrative-type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected.

If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

All of the Government's comments on deliverables shall either be incorporated in the succeeding version of the deliverable, or the contractor shall explain to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, or improper format, or otherwise does not conform to the QA requirements stated within this TO, the document may be rejected without further review and returned to the contractor for correction and resubmission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the FEDSIM COR.

E.4   DRAFT DELIVERABLES

The Government will provide written acceptance, comments, and/or change requests, if any, within 15 workdays from Government receipt of the draft deliverable. Upon receipt of the Government's comments, the contractor shall have ten workdays to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form. Software product and documentation acceptance, as previously described in the TOR, are also subject to additional IV&V testing, as needed.

E.5   WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The FEDSIM CO or FEDSIM COR will provide written notification of acceptance or rejection (Section J, Attachment A9) of all final deliverables within 15 workdays (unless specified otherwise in Section F). All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

E.6   NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. Deficiencies shall be corrected, by the contractor, within ten workdays of the rejection notice. If the deficiencies cannot be corrected within ten workdays, the contractor shall immediately notify the FEDSIM COR of the reason for the delay and provide a proposed corrective action plan within ten workdays.

If the contractor does not provide products or services that conform to the requirements of this TO, the Government may document the issues associated with the non-conforming products or services in the award fee determination report, and there may be an impact to the award fee earned.

SECTION F – DELIVERIES OR PERFORMANCE

F.1 PERIOD OF PERFORMANCE

The period of performance for this TO is a one-year base period and six, one-year options.

Base Period:	September 27, 2019 through September 26, 2020
First Option Period:	September 27, 2020 through September 26, 2021
Second Option Period:	September 27, 2021 through September 26, 2022
Third Option Period:	September 27, 2022 through September 26, 2023
Fourth Option Period:	September 27, 2023 through September 26, 2024
Fifth Option Period:	September 27, 2024 through September 26, 2025
Sixth Option Period:	September 27, 2025 through September 26, 2026

F.2 PLACE OF PERFORMANCE

The place of performance is the contractor's own facility in the Washington, D.C. metropolitan area, no more than 30 miles from CA/CST at 600 19th Street, NW, Washington, D.C.

F.3 TASK ORDER (TO) SCHEDULE AND MILESTONE DATES

The following schedule of milestones will be used by the FEDSIM COR to monitor timely progress under this TO.

The following abbreviations are used in this schedule:

DEL: Deliverable
IAW: In Accordance With
NLT: No Later Than
TOA: Task Order Award
All references to days: Government Workdays

Deliverables are due the next Government workday if the due date falls on a holiday or weekend.

Data Rights Clause - Abbreviations in the Gov't Rights column of the table below shall be interpreted as follows:

UR: Unlimited Rights, per FAR 27.404-1(a) and 52.227-14
RS: Restricted Software, per FAR 27.404-2 and 52.227-14
LD: Limited Rights Data, per FAR 27.404-2 and 52.227-14

For software or documents that may be either proprietary COTS or custom, RS/LD rights apply to proprietary COTS software or documents and UR rights apply to custom software or documents. The Government asserts UR rights to open source COTS software. Any collateral agreements (within the meaning of FAR 52.227-14) proposed for data, regardless of the type of rights offered, shall be subject to the requirements of TOR Section H.11.1 and H.11.2. For purposes of the foregoing, the terms "collateral agreement," "Supplier Agreement," and "Commercial Supplier Agreement" have the same meaning.

The Government does not assert any rights to management software tools if the contractor does not plan to charge the Government directly for that tool and does not propose that the Government will own or use that tool.

The contractor shall deliver the deliverables listed in the following table on the dates specified:

DEL. #	MILESTONE/ DELIVERABLE	CLIN	TOR REF.	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS
TASK 1 – PROJECT MANAGEMENT					
	Project Start (PS)			No later than 15 workdays after TOA	N/A
1	Kick-Off Meeting Agenda	0001	C.5.1.1	At least three workdays prior to the Kick-Off Meeting	UR
2	Kick-Off Meeting	0001	C.5.1.1	No later than five workdays after PS	N/A
3	Kick-Off Meeting Minutes Report	0001	C.5.1.1	Five workdays after the Kick-Off Meeting	UR
4	Weekly Activity Report (WAR)	X001	C.5.1.10, C.5.5.1.4	Weekly, on Mondays	UR
5	Contract Status Report (CSR)	X001	C.5.1.2, C.5.1.4	20th of the month	UR
6	CSR Status Meeting	X001	C.5.1.3	Quarterly	N/A
7	CSR Status Meeting Minutes	X001	C.5.1.3	Five workdays after CSR Status Meeting	UR
8	Draft Project Management Plan (PMP)	0001	C.5.1.1, C.5.1.5	Due at Kick-Off Meeting	UR
9	Final PMP	0001	C.5.1.5	10 workdays after receipt of Government comments	UR
10	PMP Updates	X001	C.5.1.5	As project changes occur, no less frequently than annually	UR
11	Trip Report(s)	X001	C.5.1.6	Within ten workdays following completion of each trip	UR
12	RESERVED				

DEL. #	MILESTONE/ DELIVERABLE	CLIN	TOR REF.	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS
13	Updated Baseline QMP	0001	C.5.1.1, C.5.1.5	Due at Kick-Off Meeting	UR
14	Final Baseline QMP	0001	C.5.1.5.1	10 workdays after receipt of Government comments	UR
15	QMP Updates	X001	C.5.1.5.1	As changes in program processes are identified	UR
16	Updated Transition-In Plan	0001	C.5.1.1, C.5.1.7	Due at Kick-Off Meeting	UR
17	Final Transition-In Plan	0001	C.5.1.7	10 workdays after receipt of Government comments	UR
18	Draft Transition-Out Plan	0001	C.5.1.8	Within eight months of PS	UR
19	Final Transition-Out Plan	X001	C.5.1.8	Annually, and when plans change	UR
20	Transition-Out Plan Updates	X001	C.5.1.8	At least quarterly during final Option Period	UR
21	Quarterly Spend Plan	X001	C.5.1.9	Quarterly	UR
22	Copy of TO (initial award and all modifications)	X001	F.4	Within ten workdays of award	N/A
TASK 2 – PRODUCTION SUPPORT					
23	Standard Operating Procedures	X001	C.5.1.5, C.5.2.3	IAW the PMP	UR
24	Configuration and deployment technical documents, training, source code, and other IP	X001	C.5.2.2, C.5.2.6	As required for production support	UR
TASK 3 – TIOCA PORTFOLIO MAINTENANCE					

DEL. #	MILESTONE/ DELIVERABLE	CLIN	TOR REF.	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS
25	TIOCA portfolio software maintenance and implementation technical artifacts (revised source and object code, scripts, training, user manuals, test plans and results, etc.)	X001	C.5.3, C.5.3.2	As required to provide maintenance	UR
26	Software Maintenance Releases	X001	C.5.3, C.5.3.2, C.5.3.3	As required for software maintenance releases	UR
TASK 4 – TIOCA PORTFOLIO ENHANCEMENTS					
27	TIOCA portfolio software enhancement and implementation technical artifacts (analysis, design revised source and object code, scripts, training, user manuals, test plans and results, etc.)	X001	C.5.4	As required to support enhancement	UR
28	Enhancement Requirements Analyses	X001	C.5.4	As required to support enhancement	UR
29	Software Enhancement Releases	X001	C.5.3.3, C.5.4	As required to support enhancement	UR
TASK 5 – CLASS SUPPORT					
30	Name-Checking Algorithm Documentation	X001	C.5.5.1.1	Ongoing Document Maintenance/ Revisions	UR
31	Develop, modify, deploy linguistic algorithms	X001	C.5.5.1.1, C.5.5.1.2	Ongoing Document Maintenance/ Revisions	UR

DEL. #	MILESTONE/ DELIVERABLE	CLIN	TOR REF.	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS
32	CLASS Functionality Design, Implementation, and Integration	X001	C.5.5.1.2	Ongoing	UR
33	Training, Briefings, Demonstrations	X001	C.5.5.1.3	As requested by DOS or at the time new functionality is deployed	UR

The contractor shall mark all deliverables listed in the above table to indicate authorship by contractor (i.e., non-Government) personnel; provided, however, that no deliverable shall contain any proprietary markings inconsistent with the Government's data rights set forth in this TO. The Government reserves the right to treat non-conforming markings in accordance with subparagraphs (e) and (f) of the FAR clause at 52.227-14.

F.4 PUBLIC RELEASE OF CONTRACT DOCUMENTS REQUIREMENT

The contractor agrees to submit, within ten workdays from the date of the FEDSIM CO's execution of the initial TO, or any modification to the TO (exclusive of Saturdays, Sundays, and Federal holidays), a Portable Document Format (PDF) file of the fully executed document with all proposed necessary redactions, including redactions of any trade secrets or any commercial or financial information that it believes to be privileged or confidential business information, for the purpose of public disclosure at the sole discretion of GSA (Section F, Deliverable 22). The contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 United States Code (U.S.C.) § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b)(4), shall explain why the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. Information provided by the contractor in response to the TO requirement may itself be subject to disclosure under the FOIA. Submission of the proposed redactions constitutes concurrence of release under FOIA.

GSA will carefully consider the contractor's proposed redactions and associated grounds for nondisclosure prior to making a final determination as to what information in such executed documents may be properly withheld.

F.5 DELIVERABLES MEDIA

All document deliverables shall be saved on SharePoint or ShareDrive or other Government-specified locations. In addition, all document deliverables shall be emailed to the FEDSIM COR and CA/CST GTM. Software and other technical deliverables unsuitable for Microsoft (MS) Office or PDF format shall be saved on media or servers specified by the Government and native to the software.

The table at F.4 includes deliverables and expected due dates. Document deliverables shall be provided electronically in a MS Office Suite product pre-approved by the Government, whose versions shall be compatible with the latest commonly available version on the market or as specified by CA/CST.

a.	Text	MS Word, Google Docs, PDF
b.	Spreadsheets	MS Excel, Google Sheets
c.	Briefings	MS PowerPoint, Google Slides
d.	Drawings	MS Visio, MS PowerPoint, Google Drawings
e.	Schedules	MS Project, Smartsheet

F.6 PLACE(S) OF DELIVERY

Deliverables that do not contain sensitive information shall be delivered to the FEDSIM COR at the address below. Some deliverables contain sensitive information and shall only be delivered within CA/CST's offices. The place(s) of delivery for sensitive deliverables will be identified post award.

> GSA FAS AAS FEDSIM
> ATTN: Sandy Greenwell, COR (QF0B)
> 1800 F Street, NW
> Washington, D.C. 20405
> Telephone: (703) 589-2564
> Email: sandy.greenwell@gsa.gov

Copies of all deliverables shall also be delivered to the CA/CST GTM.

F.7 NOTICE REGARDING LATE DELIVERY/PROBLEM NOTIFICATION REPORT (PNR)

The contractor shall notify the FEDSIM COR via a PNR (Section J, Attachment A10) as soon as it becomes apparent to the contractor that a scheduled delivery will be late. The contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery, and the project impact of the late delivery. The FEDSIM COR will review the new schedule and provide guidance to the contractor. Such notification in no way limits any Government contractual rights or remedies including, but not limited to, termination.

G.1 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The FEDSIM CO appointed a FEDSIM COR in writing through a COR Appointment Letter (Section J, Attachment A1). The FEDSIM COR will receive, for the Government, all work called for by the TO and will represent the FEDSIM CO in the technical phases of the work. The FEDSIM COR will provide no supervisory or instructional assistance to contractor personnel.

The FEDSIM COR is not authorized to change any of the terms and conditions, scope, schedule, and price of the contract or the TO. Changes in the scope of work will be made only by the FEDSIM CO by properly executed modifications to the Contract or the TO.

G.1.1 CONTRACT ADMINISTRATION

Contracting Officer:

> Bryan Davis Keith
> GSA FAS AAS FEDSIM (QF0B)
> 1800 F Street, NW
> Washington, D.C. 20405
> Telephone: (703) 819-5235
> Email: bryan.keith@gsa.gov

Contracting Officer's Representative:

> GSA FAS AAS FEDSIM
> ATTN: Sandy Greenwell, COR (QF0B)
> 1800 F Street, NW
> Washington, D.C. 20405
> Telephone: (703) 589-2564
> Email: sandy.greenwell@gsa.gov

Alternate Contracting Officer's Representative:

> GSA FAS AAS FEDSIM
> ATTN: Courtney Loy, Alternate COR (QF0B)
> 1800 F Street, NW
> Washington, D.C. 20405
> Telephone: (202) 615-2066
> Email: courtney.loy@gsa.gov

Government Technical Managers:

> Michael Carlo
> DOS CA/CST/PSDD/BIMS
> 600 19th Street, NW
> Washington, D.C. 20036
> Telephone: (202) 485-7785
> Email: CarloM@state.gov

Alternate Government Technical Manager:

> Sharon Westmark
> DOS CA/CST/PSDD
> 600 19th Street, NW
> Washington, D.C. 20036
> Telephone: (202) 485-7722
> Email: westmarkSB@state.gov

G.2   INVOICE SUBMISSION

The contractor shall submit Requests for Payments in accordance with the format contained in General Services Administration Acquisition Manual (GSAM) 552.232-25, Prompt Payment (NOV 2009), to be considered proper for payment. In addition, the following data elements shall be included on each invoice:

> Task Order Number: 47QFCA19F0028
>
> Paying Number: A21436666
>
> FEDSIM Project Number: 2019020SD
>
> Project Title: Travel Issuance and Overseas Citizen Assistance (TIOCA)

The contractor shall submit invoices as follows:

The contractor shall use FEDSIM's electronic Assisted Services Shared Information SysTem (ASSIST) to submit invoices. The contractor shall manually enter CLIN charges into Central Invoice Services (CIS) in the ASSIST Portal. Summary charges on invoices shall match the charges listed in CIS for all CLINs. The contractor shall submit invoices electronically by logging onto the following link (requires Internet Explorer to access the link):

> https://portal.fas.gsa.gov

Log in using the assigned Identification (ID) and password, navigate to the order against which you want to invoice, click the Invoices and Acceptance Reports link in the left navigator, and then click the *Create New Invoice* button. By using this method, no paper copy of the invoice shall be submitted to GSA FEDSIM or the GSA Finance Center. The contractor shall provide invoice backup data, as an attachment to the invoice, in accordance with the contract type, including detail such as labor categories, rates, and quantities of labor hours per labor category. The FEDSIM COR may require the contractor to submit a written "hardcopy" invoice with the client's certification prior to invoice payment. A paper copy of the invoice is required for a credit.

The contractor is certifying, by submission of an invoice in the CIS, that the invoice is correct and proper for payment.

If there are any issues submitting an invoice, contact the Assisted Acquisition Services Business Systems (AASBS) Help Desk for support at 877-472-4877 (toll free) or by email at AASBS.helpdesk@gsa.gov.

G.3 INVOICE REQUIREMENTS

The contractor shall submit a draft copy of an invoice backup in Excel to the FEDSIM COR and CA/CST GTM for review prior to its submission to ASSIST. The draft invoice shall not be construed as a proper invoice in accordance with FAR 32.9 and GSAM 532.9.

If the TO has different contract types, each shall be addressed separately in the invoice submission.

The final invoice is desired to be submitted within six months of project completion. Upon project completion, the contractor shall provide a final invoice status update monthly.

Regardless of contract type, the contractor shall report the following metadata:

    a. GWAC Contract Number.
    b. Task Order Award Number (NOT the Solicitation Number).
    c. Contractor Invoice Number.
    d. Contractor Name.
    e. POC Information.
    f. Current period of performance.
    g. Amount of invoice that was subcontracted.

The amount of invoice that was subcontracted to a small business shall be made available upon request.

G.3.1 COST-PLUS-AWARD-FEE (CPAF) CLINs (for LABOR)

The contractor may invoice monthly on the basis of cost incurred for the CPAF CLINs. The invoice shall include the period of performance covered by the invoice (all current charges shall be within the active period of performance) and the CLIN number and title. All hours and costs shall be reported by CLIN element (as shown in Section B), by contractor employee, and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

    a. Employee name (current and past employees).
    b. Employee company.
    c. Exempt or non-exempt designation.
    d. Employee Alliant 2 labor category.
    e. Current monthly and total cumulative hours worked.
    f. Direct Labor Rate.
    g. Effective hourly rate (e.g., cumulative costs/cumulative hours).
    h. Current approved billing rate percentages in support of costs billed.
    i. Itemization of cost centers applied to each individual invoiced.
    j. Itemized breakout of indirect costs (e.g., Fringe, Overhead (OH), General and Administrative (G&A) burdened costs for each individual invoiced (rollups are unacceptable)).
    k. Any cost incurred not billed by CLIN (e.g., lagging costs).

l. Labor adjustments from any previous months (e.g., timesheet corrections).
m. Provide comments for deviation more than ten percent.

All cost presentations provided by the contractor in Excel shall show indirect charges itemized by individual with corresponding indirect rates with cost center information. The invoice detail shall be organized by CLIN.

The contractor may invoice for fee after accepting the modification which includes the award fee determination and any corresponding deobligation of unearned fee. See the AFDP and SLAs in Section J, Attachments A4 and A5, and supplemental documents for additional information on the award fee determination process.

G.3.2 OTHER DIRECT COSTS (ODCs) AND TOOLS

The contractor may invoice monthly on the basis of cost incurred for the ODC and Tools CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. In addition, the contractor shall provide the following detailed information for each invoice submitted, as applicable. Spreadsheet submissions are required.

a. ODCs/Tools purchased.
b. Request to Initiate Purchase (RIP) or Consent to Purchase (CTP) number or identifier.
c. Date accepted by the Government.
d. Associated CLIN.
e. Project-to-date totals by CLIN.
f. Cost incurred not billed by CLIN.
g. Remaining balance of the CLIN.

All cost presentations provided by the contractor shall also include OH charges, G&A charges in accordance with the contractor's Defense Contract Audit Agency (DCAA) cost disclosure statement.

G.3.3 TRAVEL

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. Federal Travel Regulation (FTR) - prescribed by the GSA, for travel in the contiguous United States (U.S.).
b. Joint Travel Regulations (JTR) Volume 2, Department of Defense (DoD) Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.
c. Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

The contractor may invoice monthly on the basis of cost incurred for cost of travel comparable with the JTR, FTR, or DSSR, depending on the location of travel. The invoice shall include the period of performance covered by the invoice, the CLIN number and title. Separate worksheets, in MS Excel format, shall be submitted for travel.

CLIN Total Travel: This invoice information shall identify all <u>cumulative</u> travel costs billed by CLIN. The <u>current</u> invoice period's travel details shall include separate columns and totals and include the following:

    a. Travel Authorization Request number or identifier, approver name, and approval date.

    b. Current invoice period.

    c. Names of persons traveling.

    d. Number of travel days.

    e. Dates of travel.

    f. Number of days per diem charged.

    g. Per diem rate used.

    h. Total per diem charged.

    i. Transportation costs.

    j. Total charges.

    k. Explanation of variances exceeding ten percent of the approved versus actual costs.

    l. Indirect handling rate.

All cost presentations provided by the contractor shall also include OH charges and G&A charges in accordance with the contractor's DCAA cost disclosure statement.

G.4 TASK ORDER (TO) CLOSEOUT

The Government will unilaterally close out the TO no later than six years after the end of the TO period of performance if the contractor does not provide final DCAA rates by that time.

SECTION H – SPECIAL CONTRACT REQUIREMENTS

H.1   KEY PERSONNEL

The following are the minimum personnel who shall be designated as "Key." The Government does not intend to dictate the composition of the ideal team to perform this TO.

  a. Program Manager (PM)
  b. Quality Assurance (QA) Manager
  c. Senior IT Analyst

The Government desires that Key Personnel be assigned for the duration of the TO.

H.1.1   PROGRAM MANAGER (PM)

The contractor shall identify a PM by name who shall provide management, direction, administration, and leadership of the execution of this TO. The PM is ultimately responsible for the quality and efficiency of the TO, to include both technical issues and business processes. The PM shall be an employee of the prime contractor. This PM shall have the authority to commit the contractor's organization and make decisions for the contractor's organization in response to Government issues, concerns, questions, and comments, as well as be proactive in alerting the Government to potential contractual or programmatic issues including situations that may comprise the contractor's ability to provide services.

It is required that the PM has the following qualifications:

  a. Possesses an active Project Management Professional (PMP) Certification from the Project Management Institute (PMI) at the time of proposal Part III submission and throughout the life of this TO.
  b. Active certification in either SAFe Agilist (SA) or SAFe Government Practitioner (SGP).
  c. A minimum of three years of experience with scrum on a large scale.
  d. A minimum of one year of experience leading Continuous Integration/Continuous Delivery (CI/CD) implementation in support of DevOps.
  e. A minimum of five years of program management experience with programs of similar scope and complexity, including multiple simultaneous tasks.
  f. A current Top Secret (TS) clearance at the time of proposal submission and throughout the life of the TO.

It is desirable that the PM has the following qualifications:

  a. A minimum of three years of experience with System Development Life Cycles (SDLCs) of similar size and scope to CA/CST's.
  b. A minimum of ten years of program management experience with programs of similar scope and complexity, including multiple simultaneous tasks.
  c. A minimum of four years of managerial experience providing technical advice, organizing, planning, directing, and managing staff to ensure goals and objectives are achieved.
  d. A minimum of five years of experience with the management and supervision of employees in a variety of labor categories and skills.

H.1.2 QUALITY ASSURANCE (QA) MANAGER

It is required that the QA Manager has the following qualifications:

a. Active certification in either SA or SGP.

b. A minimum of three years of experience with scrum on a large scale.

c. A minimum of three years of experience with creating and running automated tests to enable CI and CD and/or with CI/CD implementation in support of DevOps.

d. A minimum of four years of experience in all phases of QA cycle (Waterfall and Agile).

It is desirable that the QA Manager has the following qualifications.

a. Proven expertise with Remedy, Collaborative Life Cycle Management Tools (IBM CLM), SharePoint, or similar tools.

b. A minimum of two years of experience with creating and running automated methods to deploy software products into the production environment.

c. A minimum of two years of experience of managing multiple QA analysts running multiple QA cycles.

H.1.3 SENIOR IT ANALYST

It is required that the Senior IT Analyst has the following qualifications:

a. A minimum of six years of proven experience in all phases of an SDLC (Waterfall and Agile) with systems of similar size, scope, complexity, and environments as in CST.

b. Active certification in either SA or SGP.

c. A minimum of three years of experience with scrum on a large scale.

d. A current TS clearance at the time of proposal submission and throughout the life of the TO.

It is desirable that the Senior IT Analyst has the following qualifications.

a. Experience with Collaborative Life Cycle Management (IBM CLM) or similar tools.

b. Experience with developing and decomposing epics, features, and user stories down to detailed functional and nonfunctional requirements.

c. A minimum of four years of supervision experience of technical teams of similar size and complexity as the teams for which they are proposed.

H.1.4 KEY PERSONNEL SUBSTITUTION

The contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the FEDSIM CO. Prior to using other than the Key Personnel specified in its proposal in response to the TOR, the contractor shall notify the FEDSIM CO and the FEDSIM COR of the existing TO. This notification shall be no later than ten calendar days in advance of any proposed substitution and shall include justification (including resume(s) and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance.

Substitute Key Personnel qualifications shall be equal to, or greater than, those of the Key Personnel substituted. If the FEDSIM CO and the FEDSIM COR determine that a proposed

substitute Key Person is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the contractor may be subject to default action as prescribed by FAR 52.249-6 Termination.

H.2   GOVERNMENT-FURNISHED PROPERTY (GFP)

The Government will provide the contractor with IT devices that include but are not limited to workstations, scanners, printers, and network and security devices. The Government will authorize individuals to use these devices, including provision of user IDs, passwords, operating instructions, and required training. The TIOCA contractor shall provide space and utilities for these devices in the contractor's secure facility.

The TIOCA contractor shall use these devices for software maintenance, enhancement, and ancillary tasks. The GFP includes devices necessary for the contractor to conduct unit and integration tests, and to reproduce tests conducted by other organizations, including IV&V tests. These tests are an essential part of application system maintenance and enhancements prior to deployment in production. These devices may also be needed to research complex problems arising from Tier III Help Desk tickets or from other sources, as well as for project management and office automation.

Some of these devices possess advanced technologies that ensure a high level of security for the artifacts they create. The devices or their supporting equipment will require supporting utilities such as conditioned electricity and/or cooling to be kept in working order and that the TIOCA contractor shall provide in the contractor's secure facility. Over the seven year Task Order Period of Performance, technology upgrades and changing requirements may well result in the need for replacement of printers located at the contractor's facility.

A third-party contractor will install, supply, and maintain the device hardware. The TIOCA contractor shall cooperate with DOS and third-party contractor(s) with movement, installation, supply, and device hardware maintenance. The TIOCA contractor shall cooperate with device installation to include specialized printers during Transition-In. The TIOCA contractor shall contact the maintenance contractor when needed for device repairs or maintenance.

H.3   GOVERNMENT-FURNISHED INFORMATION (GFI)

GFI is provided in Section J, Attachments A22 through A35.

H.4   SECURITY REQUIREMENTS

The association between the contractor and the Government is unclassified; however, disclosure of TO specifics is on a need-to-know basis. The Government anticipates that work under this TO will be conducted at multiple security levels. Work under this TO will require classified access up to TOP SECRET (TS).

Under this TO, contractor personnel are required to have current SECRET Personnel Security Clearances (PCLs) throughout the life of the TO. The Government will define individual event clearance requirements.

The prime contractor and any subcontractors must be able to obtain the required security clearances. The awardee must have the necessary clearances at the time of contract award. In

general, all necessary facility and employee security clearances shall be at the expense of the contractor. The contractor shall comply with all security requirements.

The contractor shall plan for attrition through careful scheduling and advance preparation and submission of clearance requests.

a. A TOP SECRET Facility Security Clearance (FCL) is required for performance throughout the life of the TO in accordance with the Department of Defense (DD) Form 254, Department of Defense Contract Security Classification Specification (Section J, Attachment A36).

b. **All contractor personnel assigned to this TO shall possess a SECRET PCL issued by the Defense Security Service (DSS) prior to TO performance or billing for time spent on TO tasks, except that the Program Manager and Senior IT Analyst Key Personnel shall possess a TOP SECRET PCL.**

c. Since it will be necessary for some contractor personnel to have access to classified material and/or to enter into areas requiring a security clearance, each contractor employee requiring such access must have an individual security clearance commensurate with the required access prior to performance. Individuals must maintain their security clearance for the duration of performance under this award.

d. The contractor shall obtain a DOS building pass for all employees performing under this award who require frequent and continuing access to DOS facilities in accordance with DOS Acquisition Regulation (DOSAR) 652.204-70 DOS Personal Identification Card Issuance Procedures.

e. Performance of this TO shall be in accordance with the attached DD Form 254, Department of Defense Contract Security Classification Specification and FAR 52.204-2 "SECURITY REQUIREMENTS."

f. Classified material received or generated in the performance of this award shall be safeguarded and disposed of in accordance with the National Industrial Security Program Operating Manual (NISPOM) (DOD 5220.22 M).

g. To successfully perform under this TO, the contractor, including all entities which comprise a joint venture and the joint venture itself, is required to hold a Final TOP SECRET FCL issued in accordance with the NISPOM, DoD 5220.22M. Should a party within the joint venture not hold an FCL, the offeror will need to demonstrate that said party will not be performing tasks under the TO which require a clearance (e.g., providing TO-required personnel).

h. To demonstrate the existence of a clearance, the offeror shall provide the following:
   1. Narrative confirmation of clearance level. A copy of the National Industrial Security System Facility Verification Notification (NISS FVN printout) is sufficient.
   2. Commercial and Government Entity (CAGE) code.
   3. Complete legal entity name and business address.

i. All building passes/ID cards shall be returned to DOS. Upon completion of this TO, all classified and/or Sensitive But Unclassified (SBU) information shall be returned to the Government.

j. Subcontracting firms must possess FCLs commensurate with their level of access. All sub-contractor DD254s shall be prepared and approved by DS/IS/IND prior to performance on contract.

k. Subsequent to TO award, DOS will conduct a formal briefing for the contractor. The purpose of the briefing will be to bring to the contractor's attention the governing documents and directives regarding all security considerations in the staffing of the project, site access, software and hardware functions, document control, and DS procedures.

l. DOS personnel will provide assistance in obtaining Annex (at 600 19th Street, NW, Washington, D.C.) and work place access during the period of TO support. Contractors must return all access control documentation and building badges to the DOS GTM at the completion of TO services.

m. In the event a personnel security clearance is rescinded for an individual assigned to this TO, the individual shall be removed from the TO and replaced. The TIOCA contractor shall notify the COR and the GTMs immediately. In addition, the contractor shall submit a Visit Authorization Request (VAR) cancellation to DS/IS/IND.

n. Security clearance requirements for the contractor to access DOS domestic or overseas information systems shall be in accordance with 12 FAM 600 (reference Web site: http://fam.state.gov - click on "FAM").

o. All personnel who resign, are transferred, terminated, or otherwise removed from the TO on the last day of work on site will be debriefed by the Information System Security Officer (ISSO) and shall turn in their DOS badge to the ISSO. The company must cancel the VAR previously sent to DS/IS/IND. Each employee under this TO is individually responsible for the protection of information and shall be required to sign an agreement (Department of State Form DS-0109, Separation Statement) regarding the confidentiality of the work performed under this TO.

p. The company FSO must send a VAR to DS/IS/IND via email to ds_ind_contractorvars@state.gov or by facsimile to 571-345-3000. Notification of VAR approvals are provided to the CA/CST GTM.

H.4.1 DEPARTMENT OF STATE PERSONAL IDENTIFICATION CARD ISSUANCE PROCEDURES

a. The contractor shall comply with the DOS Personal Identification Card Issuance Procedures for all employees performing under this TO who require frequent and continuing access to DOS facilities or information systems. The contractor shall insert this clause in all subcontracts when the subcontractor's employees will require frequent and continuing access to DOS facilities or information systems.

b. The DOS Personal Identification Card Issuance Procedures may be accessed at http://www.state.gov/m/ds/rls/rpt/c21664.htm

H.4.2 OPENNET CONNECTIVITY

The contractor will be required to establish connectivity to the Department OpenNet from the contractor facility (OpenNet Extension). The program office will sponsor the contractor for the connectivity to OpenNet.

Recent historical data indicates that OpenNet connectivity supporting application software maintenance and enhancement for the four major programs that TIOCA portfolio will now incorporate has previously been supported by network connections with a total bandwidth of 100 megabytes (MB). This bandwidth has been provided either by a new, dedicated line or by allocation of a certain amount of bandwidth from an existing connection.

    a. The contractor facility must be secured for the protection of OpenNet and SBU data. As a minimum, the facility must:

      1. Computer Room - Physical Security

        i. Perimeter walls must be of slab-to-slab construction to include the area above the false ceiling. #9 10-gauge expanded metal may be used to allow airflow through openings into the OpenNet space. The barrier must be secured from the OpenNet space.

        ii. Openings greater than 96 square inches must be protected by ½" steel bars welded 6" on center vertically and horizontally or with #9 10-gauge expanded metal.

        iii. All reverse mounted, out-swinging doors must have heavy-duty butt hinges with non-removable pins.

        iv. All reverse mounted, outward-swinging doors must have latch-guard plates installed.

        v. All entry points to the suite must be equipped with an Access Control System (ACS) that requires key-card access. Entry and exit audit records must be available for a period of not less than one year.

        vi. All monitors must face away from windows or be protected from view by opaque curtains, window shades, or screen-view filters.

        vii. There must be an approved shredder available to properly dispose of SBU information. The shredder must meet the requirements of NIST SP 800-88. The shredder must be capable of rendering hardcopy materials unreadable, indecipherable, and irrecoverable.

      2. Server Room

        i. The server room perimeter walls must extend from the structural floor to the structural ceiling.

        ii. Openings in the perimeter walls larger than 96 square inches must be screened with 9 gauge expanded metal.

        iii. The server room must be located above ground and in interior portions of the building, away from areas subject to frequent use to minimize potential damage from physical and environmental hazards.

        iv. The server room must be located away from potential sources of fire such as kitchens, main electrical power distribution panels, and storage areas for combustible materials.

b. Co-location of DOS equipment with personnel that do not possess the minimal security clearance or meet the confirmed need-to-know requirements to access Department data is prohibited.

c. Personnel (e.g., contractor staff, cleaning staff, and building maintenance staff) that do not meet the requirements in Sections H.4.b and H.4.c and meet the need-to-know requirements, but require physical access to areas where the OpenNet equipment is located, must be escorted at all times by a contractor employee that has authorized access to OpenNet.

d. All contractor personnel with access to the OpenNet must report any security incident to the contractor's Alternate Information System Security Officer (AISSO), who must report to DS/IS/IND and the contractor Facility Security Officer (FSO) in accordance 12 FAM 590, Cyber Security Incident Program.

e. All hardware and software used for this extension must be local or IT CCB-approved and configured, and managed in accordance with 12 FAM 600 and Department security configuration guidelines.

f. All media (e.g., hard drives, Compact Disks (CDs), flash memory, etc.) used on OpenNet must be returned to CST when:

    1. The media is no longer needed.

    2. The media is inoperative.

    3. The extension is no longer required by the contractor.

    4. The TO is terminated.

g. The OpenNet extension must have no other network connections.

h. All OpenNet processing areas must be approved for the protection of SBU data by DOS/IS/IND.

i. The contractor must notify DS/IS/IND when users no longer require access to OpenNet.

j. Any changes to the configuration of this extension (e.g., adding additional workstations, relocating existing workstations) or any changes to the physical structure of the OpenNet space must be approved by DS/SI/CS.

k. DS/IS/IND and the contractor must agree that the OpenNet extension is subject to on-site and remote auditing, scanning, and testing as deemed necessary by DS. This auditing, scanning, and testing will help to assess the compliance of this OpenNet extension with DOS requirements.

l. If at any time, DS finds that the above listed security requirements are not being met, the OpenNet extension will be subject to termination.

H.4.3 SENSITIVE INFORMATION AND PRIVACY

The contractor may have access to sensitive (to include privileged and confidential) data, information, and materials of the U.S. Government. These printed and electronic documents are for internal use only and remain the sole property of the U.S. Government. Some of these materials are protected by the Privacy Act of 1974 (AMENDED) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.

H.5 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS

H.5.1 ORGANIZATIONAL CONFLICT OF INTEREST (OCI)

a. If a contractor has performed, is currently performing work, or anticipates performing work that creates or represents an actual or potential OCI, the contractor shall immediately disclose this actual or potential OCI to the FEDSIM CO in accordance with FAR Subpart 9.5. The nature of the OCI may involve the prime contractor, subcontractors of any tier, or teaming partners.

b. The contractor is required to complete and sign an OCI Statement (Section J, Attachment A11). The contractor must represent either that (1) It is not aware of any facts which create any actual or potential OCI relating to the award of this TO, or (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential OCI and has included a mitigation plan in accordance with paragraph (c) below.

c. If the contractor with an actual or potential OCI believes the conflict can be avoided, neutralized, or mitigated, the contractor shall submit a mitigation plan to the Government for review.

d. In addition to the mitigation plan, the FEDSIM CO may require further information from the contractor. The FEDSIM CO will use all information submitted by the contractor, and any other relevant information known to GSA, to determine whether an award to the contractor may take place, and whether the mitigation plan adequately avoids, neutralizes, or mitigates the OCI.

e. If any such conflict of interest is found to exist, the FEDSIM CO may determine that the conflict cannot be avoided, neutralized, mitigated, or otherwise resolved to the satisfaction of the Government, and the contractor may be found ineligible for award. Alternatively, the FEDSIM CO may determine that it is otherwise in the best interest of the U.S. to contract with the contractor and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded.

H.5.2 NON-DISCLOSURE REQUIREMENTS

If the contractor acts on behalf of, or provides advice with respect to, any phase of an agency procurement, as defined in FAR 3.104-4, then the contractor shall execute and submit a Corporate Non-Disclosure Agreement (NDA) Form (Section J, Attachment A12) and ensure that all its personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the TO:

a. Are instructed in the FAR 3.104 requirements for disclosure, protection, and marking of contractor bid or proposal information, or source selection information.

b. Are instructed in FAR Part 9 for third-party disclosures when acting in an advisory capacity.

All proposed replacement contractor personnel shall also be instructed in the requirements of FAR 3.104. Any information provided by contractors in the performance of this TO or obtained from the Government is only to be used in the performance of the TO. The contractor shall put in

place appropriate procedures for the protection of such information and shall be liable to the Government for any misuse or unauthorized disclosure of such information by its personnel, as defined above.

H.6   SECTION 508 COMPLIANCE REQUIREMENTS

Unless the Government invokes an exemption, all Electronic and Information Technology (EIT) products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, 29 U.S.C. 794d, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 Code of Federal Regulations (CFR) 1194. The contractor shall identify all EIT products and services provided, identify the technical standards applicable to all products and services provided, and state the degree of compliance with the applicable standards. Additionally, the contractor must clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., Vendor's or other exact web page location). The contractor must ensure that the list is easily accessible by typical users beginning at time of award.

H.7   ADEQUATE COST ACCOUNTING SYSTEM

The adequacy of the contractor's accounting system and its associated internal control system, as well as contractor compliance with the Cost Accounting Standards (CAS), affect the quality and validity of the contractor data upon which the Government must rely for its management oversight of the contractor and TO performance. The contractor's cost accounting system shall be adequate during the entire period of performance and shall permit timely development of all necessary cost data in the form required by the TO.

H.8   RESERVED

H.9   TRAVEL

H.9.1   TRAVEL REGULATIONS

Contractor costs for travel will be reimbursed at the limits set in the FTR, JTR, and DSSR, as appropriate.

H.9.2   TRAVEL AUTHORIZATION REQUESTS (TAR)

Before undertaking travel to any Government site or any other site in performance of this TO, the contractor shall have this travel approved by, and coordinated with, the FEDSIM COR. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long-distance travel, the contractor shall prepare a TAR (Section J, Attachment A13) for Government review and approval. Long-distance travel will be reimbursed for cost of travel comparable with the FTR, JTR, or DSSR, as applicable.

Requests for travel approval shall:

a.   Be prepared in a legible manner.
b.   Include a description of the travel proposed including a statement as to purpose.
c.   Be summarized by traveler.

    d.   Identify the TO number.

    e.   Identify the CLIN associated with the travel.

    f.   Be submitted in advance of the travel with sufficient time to permit review and approval.

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

H.10 ODCS AND TOOLS

The Government may require the contractor to purchase hardware, software, and related supplies critical and related to the services being acquired under the TO. Such requirements will be identified at the time a TOR is issued or may be identified during the course of a TO by the Government or the contractor. If the contractor initiates a purchase within the scope of this TO and the prime contractor has an approved purchasing system, the contractor shall submit to the FEDSIM COR a RIP (Section J, Attachment A14). If the prime contractor does not have an approved purchasing system, the contractor shall submit to the FEDSIM CO a CTP (Section J, Attachment A15). The RIP and CTP shall include the purpose, specific items, estimated cost, cost comparison, and rationale. The contractor shall not make any purchases without an approved RIP from the FEDSIM COR or an approved CTP from the FEDSIM CO and without complying with the requirements of Section H.11.2.

H.11 COMMERCIAL SUPPLIER AGREEMENTS

H.11.1   The Government understands that commercial software tools that may be purchased in furtherance of this TO as described in Sections C.5.2.4 and as contemplated in the ODC and Tools CLINs in Section B.4 (included with final TOR) may be subject to commercial agreements which may take a variety of forms, including without limitation licensing agreements, terms of service, maintenance agreements, and the like, whether existing in hard copy or in an electronic or online format such as "clickwrap" or "browsewrap" (collectively, "Supplier Agreements"). For purposes of this TO, the Supplier Agreements are "collateral agreements" within the meaning of the FAR clause at 52.227-14.

H.11.2   The contractor shall ensure that any proposed Supplier Agreements allow the associated software and services to be used as necessary to achieve the objectives of this TO. The contractor shall provide all applicable Supplier Agreements to the FEDSIM CO prior to purchase and shall cooperate with the Government, including negotiations with the licensor as appropriate, to ensure compliance with this Section. Without limiting the generality of the foregoing, a compliant Supplier Agreement shall permit all of the following at no extra charge to the Government: (a) access and use by support contractors, including a successor contractor upon termination or expiration of this TO; (b) transfer to a different data center and/or a successor contractor's cloud; and (c) the creation of derivative works that shall be subject to at least the same rights as set forth in subparagraphs (a) and (b) above. The above rights constitute "other rights and limitations" as contemplated in subparagraph (d) of the FAR clause at 52.227-14, Rights In Data – General (May 2014), Alternate III (Dec 2007).

H.12 PRESS/NEWS RELEASE

The contractor shall not make any press/news release pertaining to this procurement without prior Government approval and only in coordination with the FEDSIM CO.

H.13 INTELLECTUAL PROPERTY RIGHTS

The existence of any patent, patent application, or other intellectual property right that encumbers any deliverable must be disclosed in writing on the cover letter that accompanies the delivery. If no such disclosures are provided, the data rights provisions in FAR 52.227-14 apply.

H.14 AWARD FEE

See the AFDP and SLAs in Section J, Attachments A4 and A5.

I.1   TASK ORDER CLAUSES

All applicable and required clauses set forth in FAR 52.301 automatically flow down to all Alliant 2 TOs, based on their specific contract type (e.g., cost, fixed-price, etc.), performance work statement, competition requirements, commercial or not commercial, and dollar value as of the date the TO solicitation is issued.

I.2   FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This TO incorporates one or more clauses by reference with the same force and effect as if they were given in full text. Upon request, the FEDSIM CO will make their full text available. Also, the full text of a clause may be accessed electronically at the FAR website:

http://www.acquisition.gov/far/

FAR	TITLE	DATE
52.203-13	Contractor Code of Business Ethics and Conduct	OCT 2016
52.203-14	Display of Hotline Poster(s) https://www.stateoig.gov/system/files/hotlineposter_stateoig.pdf	OCT 2016
52.203-17	Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights	APR 2014
52.204-2	Security Requirements	AUG 1996
52.204-9	Personal Identity Verification of Contractor Personnel	JAN 2011
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards	OCT 2016
52.204-13	System for Award Management Maintenance	OCT 2016
52.204-14	Service Contract Reporting Requirements	OCT 2016
52.204-18	Commercial and Government Entity Code Maintenance	AUG 2020
52.204-21	Basic Safeguarding of Covered Contractor Information Systems	JUN 2016
52.204-23	Prohibition On Contracting For Hardware, Software, And Services Developed Or Provided By Kaspersky Lab And Other Covered Entities	JUL 2018
52.215-21	Requirements for Certified Cost or Pricing Data and Data Other than Certified Cost or Pricing Data—Modifications	OCT 2010
52.215-23	Limitations on Pass-Through Charges	OCT 2009
52.216-7	Allowable Cost and Payment Fill-in: 30 days	JUN 2013
52.219-8	Utilization of Small Business Concerns	NOV 2016
52.223-15	Energy Efficiency in Energy Consuming Products	DEC 2007
52.224-1	Privacy Act Notification	APR 1984
52.224-2	Privacy Act	APR 1984
52.225-13	Restrictions on Certain Foreign Purchases	JUN 2008

FAR	TITLE	DATE
52.227-14	Rights in Data – General	MAY 2014
52.227-14	Rights In Data –Alternate II	DEC 2007
52.227-14	Rights In Data – Alternate III	DEC 2007
52.232-18	Availability of Funds	APR 1984
52.232-20	Limitation of Cost	APR 1984
52.232-22	Limitation of Funds	APR 1984
52.232-40	Providing Accelerated Payments to Small Business Subcontractors	DEC 2013
52.237-3	Continuity of Services	JAN 1991
52.239-1	Privacy or Security Safeguards	AUG 1996
52.244-6	Subcontracts for Commercial Items	JAN 2017
52.245-1	Government Property	JAN 2017
52.246-5	Inspection of Services - Cost-Reimbursement	APR 1984
52.246-25	Limitation of Liability – Services	FEB 1997
52.247-67	Submission of Transportation Documents for Audit Fill-in: COR, see Section G	FEB 2006
52.249-6	Termination (Cost-Reimbursement)	MAY 2004
52.249-14	Excusable Delays	APR 1984
52.251-1	Government Supply Sources	APR 2012

I.2.1 FAR CLAUSES INCORPORATED BY FULL TEXT

FAR 52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (AUG 2020)

(a) *Definitions*. As used in this clause—
Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

Covered foreign country means The People's Republic of China.
Covered telecommunications equipment or services means–

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);
(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology means–

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

   (i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

   (ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Reasonable inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

Roaming means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) *Prohibition.*

(1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) *Exceptions.* This clause does not prohibit contractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement.

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if

known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

FAR 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed six months. The Contracting Officer may exercise the option by written notice to the contractor within 30 days.

(End of clause)

FAR 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

a. The Government may extend the term of this contract by written notice to the contractor within 30 days; provided that the Government gives the contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

b. If the Government exercises this option, the extended contract shall be considered to include this option clause.

c. The total duration of this contract, including the exercise of any options under this clause, shall not exceed 90 months.

(End of clause)

I.3 GENERAL SERVICES ADMINISTRATION ACQUISITION MANUAL (GSAM), CLAUSES INCORPORATED BY REFERENCE

The full text of a clause may be accessed electronically at the GSAM website:

https://www.acquisition.gov/gsam/gsam.html/

GSAM	TITLE	DATE
552.204-9	Personal Identity Verification Requirements	OCT 2012
552.232-25	Prompt Payment	NOV 2009

GSAM	TITLE	DATE
552.232-39	Unenforceability of Unauthorized Obligations (FAR Deviation)	FEB 2018
552.232-78	Commercial Supplier Agreements Unenforceable Clauses	FEB 2018
552.239-70	Information Technology Security Plan and Security Authorization	JUN 2011
552.239-71	Security Requirements for Unclassified Information Technology Resources	JAN 2012

I.3.1   GSAM CLAUSES INCORPORATED BY FULL TEXT

GSAM 552.212-71 CONTRACT TERMS AND CONDITIONS APPLICABLE TO GSA ACQUISITION OF COMMERCIAL ITEMS (JUNE 2016)

(a) The contractor agrees to comply with any clause that is incorporated herein by reference to implement agency policy applicable to acquisition of commercial items or components. The clause in effect based on the applicable regulation cited on the date the solicitation is issued applies unless otherwise stated herein. The clauses in paragraph (b) of this section are incorporated by reference:

(b) Clauses.

552.203-71 Restriction on Advertising

552.215-70 Examination of Records by GSA

(End of clause)

I.4   HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12 (HSPD-12) AND DOS ACQUISITION REGULATION (DOSAR) 652.204-70

The contractor shall comply with the DOS Personal Identification Card Issuance Procedures for all employees performing under this contract who require frequent and continuing access to DOS facilities or information systems.

Homeland Security Presidential Directive 12 (HSPD-12) requires Federal agencies to develop and deploy for their contract personnel and employees a Personal Identity Verification (PIV) credential that is secure, reliable, and interoperable among all Federal agencies (NIST 800-116). HSPD-12 mandates the establishment of a Government-wide standard for identity credentials to improve physical security in Federally controlled facilities. To that end, HSPD-12 requires all Government employees and contractors be issued a new identity credential based on the Federal Information Processing Standard Publication (FIPS) 201 on PIV. FIPS 201 is a U.S. Federal Government standard that specifies PIV requirements for Federal employees and contractors. Following FIPS 201, this credential is referred to herein as a PIV Card.

HSPD-12 explicitly requires the use of PIV Cards "in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems." In response to HSPD-12, the NIST Computer Security Division initiated a new program for improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems. FIPS 201 was developed to satisfy the technical requirements of HSPD-12, approved by the Secretary of Commerce, and issued on February 25, 2005.

All contractor personnel shall meet a minimum vetting standard and an ID must be issued for physical and logical access.

References:

    a. http://www.state.gov/m/ds/rls/rpt/c21664.htm

    b. HSPD-12

    c. FIPS 201-2

    d. NIST SPs

The DOS Personal Identification Card Issuance Procedures may be accessed at: http://www.state.gov/m/ds/rls/rpt/c21664.htm

J.1 LIST OF ATTACHMENTS

The following attachments will be available as stated.

ATTACHMENT	TITLE
A1	COR Appointment Letters
A2	Acronyms and Abbreviations
A3	Incremental Funding Chart (electronically attached .xls)
A4	Award Fee Determination Plan (AFDP) – Rev 03
A5	Service Level Agreements (SLAs) - Rev 01
A6	Contract Status Report (CSR) Template
A7	Weekly Activity Report (WAR) Template
A8	Trip Report Template
A9	Deliverable Acceptance-Rejection Report Template
A10	Problem Notification Report (PNR)
A11	Organizational Conflict of Interest (OCI) Statement
A12	Corporate Non-Disclosure Agreement (NDA)
A13	Travel Authorization Request (TAR) Template
A14	Request to Initiate Purchase (RIP) Template (electronically attached .xls)
A15	Consent to Purchase (CTP) Template (electronically attached .xls)
A16	Reserved
A17	Reserved
A18	Reserved
A19	Reserved
A20	Reserved
A21	Reserved
A22	Reserved
A23	Reserved
A24	Reserved
A25	Reserved
A26	Reserved
A27	Reserved
A28	Reserved
A29	Reserved
A30	Reserved
A31	Reserved
A32	Reserved
A33	Reserved
A34	Reserved
A35	Reserved

A36	DD254 – Revision 1
A37	Representation Regarding Covered Telecommunications and Video Surveillance